BITCOIN



LA MONEDA DEL FUTURO

Qué es, cómo funciona y por qué cambiará el mundo

2da EDICIÓN

Bitcoin

La moneda del futuro

QUÉ ES, CÓMO FUNCIONA

Y POR QUÉ CAMBIARÁ EL MUNDO

elBitcoin.org



1ra. edición publicada en Junio de 2012.

2da. edición publicada en Enero de 2013.

Diseño de portada: Eduardo Gutiérrez García.

Para más información: *http://elbitcoin.org/contactanos/*

ACEPTAMOS DONACIONES



1Q4KHiT35UQE2KvZZMbuTBbagjqDgfqj78

A Satoshi Nakamoto

Contenido

PRÓLOGO

El patrón oro de Internet

"Si la moneda es buena, no es necesario el curso forzoso para que la gente la acepte. Y si no es buena… ¿Qué clase de tirano obligaría a su pueblo a aceptarla?"

En los últimos años hemos sido testigos de revoluciones tecnológicas que se suceden a un ritmo cada vez más acelerado, casi sin dejarnos tiempo para reflexionar sobre su impacto: internet, los teléfonos móviles, el correo electrónico, etc. Sin embargo, hay algunas ideas cuya capacidad para cambiar el mundo es tan abrumadora que cuando las descubres no puedes sino pararte a pensar. Cuando leí por primera vez sobre Bitcoin en septiembre de 2010, mi interés solo se veía superado por mi escepticismo. ¡No era posible que Bitcoin fuese todo lo que decía ser! Yo ya había sido testigo de varios intentos de crear monedas electrónicas o monedas alternativas y había visto cómo fracasaban múltiples proyectos y cómo los que tenían éxito sucumbían ante los ataques de los reguladores, a menudo espoleados por los poderosos intereses del orden establecido de la banca, las finanzas, los monopolios monetarios y los anticuados sistemas de pagos tradicionales. Las barreras de entrada eran demasiado gran des y los intereses creados demasiado fuertes para permitir una competencia real. Bitcoin era demasiado bueno para ser verdad.

Me equivocaba. Satoshi Nakamoto había creado algo capaz de revolucionar el dinero tanto como el correo electrónico había revolucionado las comunicaciones.

El Dinero es una institución social de vital importancia. En una sociedad compleja no se puede organizar la actividad económica sin una unidad de cuenta, reserva de valor y medio de intercambio. La virtud de una moneda está en cómo de bien cumple esas tres funciones. Sin una unidad monetaria estable e independiente, no pueden sobrevivir los derechos de propiedad. Sin derechos de propiedad, no sería posible el comercio, el ahorro y la inversión. Y por último, sin comercio, ahorro e inversión, se paralizaría la acumulación de

capital, que es la base de todo el progreso de la humanidad. En definitiva, no puede haber un mercado libre sin una moneda sana. En ausencia de un mercado libre, la Libertad no se ría más que un mero concepto filosófico. Para ejercer nuestra libertad en un mundo material se requiere la propiedad privada de los bienes de producción. Es decir, se requiere que las personas puedan controlar sus propias vidas.

Ya en 1609, el Padre Juan de Mariana, en su De monetae mutatione, hizo una distinción entre la moneda sana y aquella que no lo era, entre el buen dinero y el mal dinero.

"...como el cimiento del edificio debe ser firme y estable, así los pesos, medidas y moneda [no] se deben mudar, porque no bambolee y se confunda todo el comercio."

En otras palabras, alterar el valor del dinero es tan nocivo para la economía como lo sería alterar el valor de un centímetro para la ingeniería o el valor de un grado de temperatura para la química. Pero es que, además de ser nocivo para la economía, el comercio y la estabilidad, alterar el valor del dinero es un acto de puro robo, latrocinio o apropiación indebida. Las devaluaciones no se suelen hacer por teorías académicas, sino que están impulsadas por los inmediatos y prácticos beneficios que puede obtener el emisor a costa de los demás, ya sean el Rey o el César acuñando moneda envilecida para quedarse con el metal precioso sobrante, el Gobierno imprimiendo billetes para pagar sus gastos o el Banco Central creando dinero electrónico de la nada para financiar el déficit y los rescates bancarios. Siempre hay alguien que gana y alguien que pierde.

Por desgracia, la historia monetaria del siglo XX se caracteriza por el olvido generalizado de esta lección. La primera Guerra Mundial trajo consigo el abandono del patrón oro y, con él, todo tipo de excesos monetarios que no se veían en Europa desde la inflación de los Assignats durante la Revolución Francesa. Los observadores más astutos no tuvieron ningún problema a la hora de señalar la consecuencia inevitable de estos excesos. En 1919, John Maynard Keynes escribió en su libro Las Consecuencias económicas de la paz:

"Según Lenin, la mejor forma de destruir el sistema capitalista es envileciendo la moneda. No hay forma más sutil y segura de derrumbar los cimientos de la sociedad que devaluando la moneda. Es un proceso que

encauza todas las fuerzas invisibles de las leyes económicas hacia la destrucción, y lo hace de forma que ni un hombre entre un millón es capaz de diagnosticarlo.”

Lo cual es bastante irónico, ya que, siendo conscientes de esto, Keynes y sus seguidores se han convertido desde entonces en los mayores defensores de la inflación y el envilecimiento de la moneda, mientras que Lenin volvió en 1922 al patrón oro (con los chervonets) como única forma de devolver la confianza a la moneda de la URSS tras sufrir las horribles consecuencias de todas las políticas monetarias que hoy llamamos *keynesianas*.

Sin embargo, la gran virtud del patrón oro no fue la estabilidad que trajo, ni cómo esta estabilidad favoreció el crecimiento, la inversión y la prosperidad (hasta el punto en que muchos autores lo consideran una de las bases de la Revolución Industrial). La gran virtud del patrón fue que se adoptó de forma voluntaria. En 1717, Sir Isaac Newton, como Director de la Casa de la Moneda, estableció lo que hoy conocemos como el patrón oro clásico, de la misma manera en que más tarde «establecería» la Ley de la Gravedad: reconoció algo que ya existía y le dio nombre. El oro y la plata ya se aceptaban casi universalmente como moneda desde tiempos ancestrales.

Como aficionado a la criptografía y gran matemático, Newton habría apreciado inmediatamente las cualidades de Bitcoin.

Bitcoin tiene muchas virtudes, y su diseño permite entrever que detrás hay un gran conocimiento de la Historia Económica y una gran sabiduría sobre la naturaleza del ser humano y de cómo éste reacciona ante los incentivos. Bitcoin es un medio de intercambio excepcional, una unidad de cuenta superlativa y tiene el potencial de ser una reserva de valor inigualable. El libro que tenéis en vuestras manos analiza en detalle todas estas virtudes. Sin embargo, a mí me gustaría resaltar la que es, en mi humilde opinión, la más importante de todas: Bitcoin es una moneda voluntaria.

El siglo XX ha sido el siglo del dinero fiat, de los monopolios, de las guerras mundiales y de los bancos centrales. El dinero ha pasado de ser una herramienta de liberación, comercio y progreso, a ser un instrumento de control al servicio de mastodónticos y omnipresentes Estados.

Aún podemos decidir cómo será el siglo XXI. Podemos seguir la senda de la

centralización y la tiranía hasta sus últimas consecuencias lógicas. En la esfera monetaria, esto significaría un Banco Central Mundial y una moneda única, forzosa, monopolística. O podemos escoger la libertad, la descentralización y la democracia del mercado. La libertad individual de escoger qué moneda utilizar porque nos convencen sus virtudes, no porque nos obligan a utilizarla a punta de pistola o bajo la amenaza de la ley. Una moneda voluntaria debe utilizar la razón y la persuasión para tener éxito. Debe presumir de sus virtudes y demostrar ser mejor que las alternativas.

El dinero fiat, en cambio, requiere tan sólo el uso de la fuerza, las amenazas y la coacción. Siendo generosos y atribuyendo buenas intenciones a sus gestores (llamarlo «dinero fiduciario» ya es ser generoso), el dinero fi at requiere la confianza de todos los que lo utilizan. Confianza en que aquellos que lo controlan no se excederán en sus manipulaciones. Confianza en que los gobernantes cumplirán sus promesas y pagarán sus deudas.

Fueron Milton Friedman y Anna Schwartz quienes abogaron por combatir la discrecionalidad y los excesos de los banqueros centrales atándoles las manos con una regla matemática por la cual la masa monetaria debía crecer a un porcentaje fijo cada año: la llamada Regla del Porcentaje «k». Los economistas de la Escuela Austriaca le respondieron diciendo que eso era precisamente lo que, de forma orgánica, ya hacía el patrón oro… ¡Y sin necesidad de un Banco Central! Pues bien, Bitcoin combina las virtudes de ambas posturas. El papel de la minería en la producción del dinero se sustituye por analogía, ya que la labor de los «mineros» de Bitcoin es asegurar la integridad y seguridad de la red descentralizada que da vida a esta moneda. La arbitrariedad y la política se eliminan de la política monetaria. Tanto la inflación como la deflación de Bitcoin son conocidas de antemano y todos los miembros de la red están en igualdad de condiciones. Bitcoin hace innecesarios a los bancos centrales. Quizás por eso el BCE ya le presta atención como demostró en su estudio de octubre de 2012 sobre monedas virtuales titulado Virtual Currency Schemes, que parece un monográfico sobre Bitcoin.

Satoshi tuvo la genial idea de crear una moneda que no requiere la confianza para funcionar, que no puede ser controlada ni convertirse en un instrumento de control. Al igual que el oro, Bitcoin no es deuda. No representa una obligación de nadie ni una promesa que pueda romperse. Al igual que el dinero metálico,

Bitcoin permite preservar la privacidad, dejando esa decisión en manos de su dueño. A diferencia de un billete o una cuenta corriente en un banco, un bitcoin es propiedad de su dueño y solo de él, sin intermediarios, ni gobiernos, ni bancos centrales. Bitcoin es el patrón oro de internet.

El euro, el dólar y el yen, tal y como los conocemos hoy, acabarán des apareciendo. El sistema de dinero fiat, inaugurado por Nixon en 1971, se derrumbará como se han derrumbado siempre experimentos similares una y otra vez a lo largo de la Historia. Si sus guardianes actúan de forma responsable, aún puede que dure unos años, o quizás alguna década más. Pero, si no lo hacen, veremos el hundimiento pronto. De hecho, desde 2007 ya se tambalea.

Hasta hace poco, el único refugio, la única alternativa posible, era volver al pasado y a los metales preciosos. El oro y la plata han sobrevivido milenios como moneda y eso difícilmente cambiará. Hoy me atrevería a decir que Bitcoin también sobrevivirá y que no sólo ayudará a la Humanidad a sobrellevar las convulsiones causadas por los aprendices de mago al mando de los bancos centrales, sino que hará del mundo un lugar mejor. La mera existencia de una alternativa tan fácil y práctica hace que los monopolistas intenten tratar mejor a sus clientes-súbditos, dado que incluso el más aborregado de los esclavos puede comenzar a hacerse preguntas cuando ve a su hermano disfrutar de la libertad.

Este magnífico libro explica de forma sencilla, directa y elocuente las virtudes de Bitcoin. Nuestros amigos de elBitcoin.org han hecho una gran labor dando a conocer Bitcoin en el mundo hispanohablante, que tantas malas experiencias ha tenido con la mala moneda. Si quieres saber más sobre cómo funciona Bitcoin y por qué tiene tanto que ofrecer, este es el mejor sitio por dónde empezar.

La próxima vez que oigas una queja sobre la inflación, los bancos, el crédito o los tipos de interés… habla de Bitcoin. Ya no hay que esperar a que los políticos se vuelvan honrados por intervención divina. La alternativa monetaria está al alcance de nuestra mano y sólo hay que tener el valor de actuar.

Félix Moreno de la Cova

Madrid, 2013

INTRODUCCIÓN

El 19 de Junio de 2010 descubrimos a Bitcoin. Lo sabemos porque fue ese el día en que publicamos una entrada de blog anunciando la buena nueva: ya está entre nosotros la primera "moneda digital descentralizada" – concepto que, a decir verdad, todavía no alcanzábamos a comprender del todo. Apenas conocíamos el significado de la palabra "criptografía", así que el funcionamiento de Bitcoin era poco menos que un misterio para nosotros. El fascinante *paper* de Bitcoin, escrito por un tal Satoshi Nakamoto, nos había dejado más preguntas que respuestas. Sin embargo, leyéndolo tuvimos una corazonada; intuimos que algo grande se estaba gestando… y lo dimos a conocer. La entrada fue breve y contundente:

"Con ustedes, ¡Bitcoin!, la primera moneda digital basada en una red peer-to-peer.

Recordemos que sin dinero de curso forzoso casi ningún Estado podría financiarse hoy en día. Y tengamos en cuenta que, salvo eliminando Internet, parece imposible frenar este tipo de innovaciones...

¿Será el principio del fin de la mayor estafa de la historia?"

En aquél entonces, cada bitcoin cotizaba aproximadamente a 0,005 dólares. Lejos estaban aún los artículos acerca de Bitcoin en medios masivos de comunicación, los sitios de intercambio de bitcoins por otras monedas, los debates acerca de la viabilidad del sistema, la fiebre de la minería Bitcoin, el aumento parabólico del precio, los robos, la explosión de emprendimientos relacionados con Bitcoin, las conferencias internacionales...

Recién en Marzo de 2011 volvimos a prestarle atención a aquél asunto de la

moneda *peer-to-peer*, justo cuando la historia estaba a punto de empezar a desplegarse. Las palabras de Gavin Andresen (líder actual del proyecto Bitcoin) en una entrevista radial despertaron en nosotros nuevamente aquella sensación de estar ante un fenómeno de consecuencias económicas y sociales muy profundas. Pero fue tras leer prácticamente todo el material disponible acerca del tema que nos convencimos de estar asistiendo a los preludios de un cambio radical, comparable al que dio lugar en el siglo XV la imprenta de Gutenberg.

Es normal que nuestras afirmaciones parezcan un tanto exageradas; al fin y al cabo, los saltos evolutivos no son precisamente frecuentes. Por eso hemos decidido reunir en este libro todas las razones que explican por qué habrá un antes y un después de Bitcoin; por qué Bitcoin actúa como una fuerza liberadora y por qué Bitcoin será ubicuo en un futuro no lejano, tal como lo es Internet en la actualidad.

Hoy, a más de dos años de aquella primera aproximación al concepto de una moneda digital descentralizada, y más de un año después de habernos abocado a la divulgación del tema en idioma español, nuestro entusiasmo sigue creciendo. Si te preguntas por qué, simplemente sigue leyendo y encontrarás la respuesta.

Esperamos que disfrutes de esta selección de artículos, ensayos, entrevistas y tutoriales. Tus comentarios serán muy bienvenidos en *http://elbitcoin.org/contactanos/*

PRIMERA PARTE

LAS BASES: DISEÑO Y DESIGNIO DE BITCOIN

I - Qué es bitcoin y cómo funciona

Un camino no recorrido

Si bien la moneda nació como una institución liberadora y promotora de la cooperación entre los seres humanos, con el tiempo los gobiernos han logrado convertirla en una herramienta de control social cada vez más sofisticada. Es por eso que todos los emprendedores involucrados en la creación de monedas de uso voluntario – es decir no impuestas por la fuerza – se han tenido que enfrentar al largo brazo de la ley (bien armado, por cierto).

Entre el tendal de víctimas podemos encontrar al Liberty Dólar y a su creador, Bernard von NotHaus, quien sufriera una redada por parte del FBI en la que se confiscaron todos sus activos (el oro y la plata que respaldaban dicha moneda), y quien fuera luego condenado a prisión. Otros casos conocidos son los de eGold (compañía que solía permitir la transferencia de letras digitales con respaldo en oro, también arruinada por el gobierno de los EE.UU) y Goldmoney (compañía que aún resiste el acoso del gobierno de los EE.UU, y que ha sido obligada a cancelar su servicio en varios países, y a cancelar su sistema de pagos en línea en todas partes).

Pero Bitcoin ha llegado para cambiar las reglas del juego. Este increíble ejemplo de ingenio y visión reúne todas las cualidades deseables en un medio de intercambio indirecto (dinero), y está libre de aquellos problemas que a menudo limitan las ventajas de tan importante herramienta, a saber: elevados costos de traslado y transacción, exposición a violaciones de la seguridad y la privacidad, posibilidad de expansión crediticia con fines políticos (causa principal del ciclo económico) e inflación (pérdida del poder adquisitivo) por aumento discrecional de la masa monetaria, entre otras muchas distorsiones derivadas de la intervención gubernamental. Veamos en detalle de qué se trata…

Generalidades

Bitcoin es una moneda electrónica descentralizada, concebida en 2009 por

quien se ha dado a conocer como Satoshi Nakamoto (aunque su verdadera identidad se desconoce). El nombre Bitcoin se aplica también al software libre diseñado por Nakamoto para la gestión de dicha moneda, y a la red P2P (*peer to peer*, o red de "pares" bajo un mismo protocolo) que le da soporte. A diferencia de la mayoría de las monedas, el funcionamiento de Bitcoin no depende de una institución central, sino de una base de datos distribuida. El software ideado por Nakamoto emplea la criptografía para proveer funciones de seguridad básicas, tales como la garantía de que los bitcoins sólo puedan ser gastados por su dueño, y nunca más de una vez.

Bitcoin es una de las primeras implementaciones del concepto de criptomoneda, y sin duda la más exitosa hasta la fecha. La propuesta que inspiró a Nakamoto – de una forma de dinero electrónico imposible de monopolizar, irrastreable y que les permite a sus dueños mantenerse anónimos – fue descripta por primera vez en 1998 por el criptógrafo Wei Dai en la célebre lista de correo electrónico Cypherpunk. El diseño de Bitcoin, de hecho, permite poseer y transferir valor entre cuentas públicas de forma potencialmente anónima.

Quizás el mayor logro de Satoshi Nakamoto sea el de haber resuelto el problema del doble gasto en un sistema descentralizado, que tanto ha desvelado a economistas y programadores. Para evitar que un mismo bitcoin sea gastado más de una vez por la misma persona (en otras palabras, para evitar la falsificación), la red se vale de lo que Nakamoto describe como un *servidor de tiempo distribuido*, que identifica y ordena secuencialmente las transacciones e impide su modificación. Esto se logra por medio de pruebas de trabajo encadenadas (las cuales se muestran como "confirmaciones"). Más adelante veremos que dicho trabajo es realizado por los ¨mineros de bitcoins¨ a cambio de una recompensa en bitcoins.

Si bien el envío de bitcoins es instantáneo, y cualquier operación puede ser monitoreada en tiempo real, las confirmaciones que nos muestra la pantalla cuando usamos el software de Bitcoin vienen a representar el proceso de ¨*clearing*¨. A mayor número de confirmaciones, más remota será la posibilidad de ser víctima de un doble gasto. Cuando supera las cinco confirmaciones por parte de la red, una transacción es considerada técnicamente irreversible.

Seguridad

Cabe destacar que, hasta la fecha, no se ha documentado ningún caso de doble gasto, pero es cierto que un ataque informático de este tipo es teóricamente posible, siempre y cuando el atacante controle al menos el 51% del poder computacional que protege a la red. Sin embargo, engañar a la red el tiempo suficiente como para llevar a cabo un único doble gasto implicaría una inversión tan descomunal (el poder de cómputo de la red Bitcoin es varias veces superior al de las 100 supercomputadoras más rápidas que existen, todas combinadas), y una organización tan compleja, que desde un punto de vista económico sería infinitamente más provechoso poner esos recursos a trabajar bajo las reglas del protocolo Bitcoin. Por otra parte, el código ha sido recientemente modificado para facilitar la detección y neutralización de este tipo de ataques – sean cuales sean sus motivaciones.

La inmensa mayoría de los que aceptan bitcoins se conforman con una única confirmación. Para montos pequeños es razonable, incluso, aceptar transacciones instantáneamente – antes de que sean confirmadas por la red.

La información que habilita el control de los bitcoins que uno posee puede ser guardada en cualquier soporte de información digital (disco rígido personal, tarjeta o llave de memoria, CD, casilla de web-mail, etc.) en la forma de un archivo "billetera", o bien custodiada por sitios web que ofrecen "cuentas Bitcoin". También es posible mantener dicha información en soportes no digitales (impresa en papel, por ejemplo) y hasta en el propio cerebro. La posesión de los bitcoins puede ser transferida por medio de Internet a cualquiera que tenga una "dirección Bitcoin", a semejanza de la manera en que se envía un e-mail a una dirección de correo electrónico.

Según los expertos, gracias a la arquitectura criptográfica de Bitcoin una transferencia entre direcciones Bitcoin es varias veces más segura que una transferencia entre cuentas bancarias (sin contar el riesgo que implica la forzosa intromisión de terceros en el sistema bancario).

En resumen

Puede decirse que Bitcoin funciona como un libro contable descentralizado, en el cual los saldos no están ligados a los usuarios sino a las direcciones

públicas que ellos controlan. El historial de todos los movimientos de bitcoins permanece almacenado en la cadena de bloques, una base de datos distribuida que mantiene el registro de todas las transacciones en cada uno de los múltiples nodos que integran la red (ver más adelante “Cadena de bloques”). Estos nodos no son más que computadoras ejecutando el software de Bitcoin en todo el mundo, conectadas entre sí por medio de Internet.

La naturaleza P2P de la red Bitcoin hace imposible el establecimiento de un control centralizado de todo el sistema. Esto impide el aumento arbitrario de la cantidad de bitcoins en circulación (lo que generaría inflación) y cualquier otro tipo de manipulación del valor por parte de las autoridades.

Información técnica

Los principios del sistema están detallados en el Paper de Bitcoin, escrito en el año 2008 por Satoshi Nakamoto.

Direcciones

Cualquier persona que participa en la red Bitcoin posee una billetera electrónica que contiene pares de llaves criptográficas. Las *direcciones* Bitcoin visibles derivan de las llaves públicas de cada usuario, y a su vez funcionan como los puntos *remitente*/*receptor* para todos los pagos. Las llaves privadas correspondientes a cada llave pública sirven para que un determinado usuario autorice pagos (transfiera bitcoins) desde su billetera.

Las direcciones públicas no tienen ninguna información sobre sus dueños; éstas aparecen como secuencias aleatorias de números y letras de 33 caracteres de largo, como por ejemplo:

1Q4KHiT35UQE2KvZZMbuTBbagjqDgfqj78

Los usuarios de Bitcoin pueden tener múltiples direcciones; de hecho, pueden generar direcciones nuevas fácilmente y sin límites. Generar una nueva dirección equivale a generar un nuevo par de llaves (pública/privada), y no requiere ningún contacto con nodos de la red. Los usuarios que desean preservar el anonimato suelen crear una nueva dirección para cada transacción.

Transacciones

Cuando un usuario ***A*** transfiere bitcoins a un usuario ***B***, el usuario ***A*** renuncia a su posesión de un determinado número de bitcoins, agregándoles la llave pública de ***B*** y firmando la combinación resultante con su llave privada. (Gracias al empleo de la criptografía asimétrica, la llave privada no puede ser deducida de la firma que de ella deriva). Esta información se transmite a toda la red *P2P* como una nueva *transacción*. Entonces, el resto de los nodos de la red verifican el número de bitcoins involucrados y la autenticidad de las firmas criptográficas, antes de aceptar la transacción como válida.

Cadena de bloques

Cualquier transacción transmitida a otros nodos no se convierte inmediatamente en "oficial"; primero tiene que ser confirmada en una lista – mantenida colectivamente – de todas las transacciones conocidas: la *cadena de bloques*. Tal es el trabajo de los "*nodos generadores*", cuyos dueños son los "*mineros de bitcoins*".

Cada nodo generador de bitcoins recoge todas las transacciones que aún no fueron confirmadas en un archivo (el bloque candidato) que contiene la referencia a dichas transacciones y al último bloque válido conocido por ese nodo. Entonces, los nodos generadores compiten entre sí tratando de encontrar un hash de ese bloque (un código aleatorio que lo representa), en un esfuerzo computacional que demanda cantidades predecibles de intento y error. Cuando un nodo encuentra la solución, la transmite a toda la red. El resto de los nodos reciben el nuevo bloque solucionado, lo verifican antes de aceptarlo y lo agregan a la cadena.

Aunque ningún usuario de Bitcoin está forzado a revelar su identidad, todas las transacciones jamás realizadas quedan grabadas en esa base de datos de libre acceso que es la cadena de bloques. Esta contiene el historial de posesión de todas las monedas (o fracciones de monedas), desde la dirección creadora hasta la dirección del actual dueño, y se encuentra en todas las computadoras que ejecutan el software de Bitcoin. Por lo tanto, si un usuario intenta reutilizar monedas que él mismo ya gastó (doble gasto), la red lo detectará y rechazará la transacción.

La cadena de bloques es un registro totalmente transparente: cualquiera puede examinarla, en cualquier momento, para informarse acerca de cualquier transacción que se haya realizado desde el lanzamiento de Bitcoin, así como de las nuevas transacciones que se van agregando a la cadena en tiempo real. Varios servicios facilitan este tipo de monitoreo.

CÓMO SE GENERAN LOS BITCOINS

Aproximadamente seis veces por hora, la red Bitcoin crea y distribuye un lote de nuevos bitcoins a quien que esté ejecutando el software para generar bitcoins (*software* de "minería"). Generar bitcoins es conocido como

“minar”, un término que remite a la minería de metales preciosos. La probabilidad de que un usuario reciba un lote depende del poder computacional con el que contribuye a la red en relación al poder computacional de todos los otros nodos combinados.

El primer nodo generador en encontrar la solución al problema criptográfico que presenta el bloque-candidato es el que obtiene un nuevo lote de bitcoins. Los “mineros” también pueden unirse por medio de Internet para generar bitcoins en grupo, formando un “pool minero”.

La cantidad de bitcoins creada por lote nunca es ni será mayor a 50 BTC, y los premios (el número de bitcoins por lote) están programados para disminuir con el paso del tiempo, reduciendo el incremento de la masa monetaria de manera predecible, hasta llegar a cero. Nunca llegarán a existir más de 21 millones de bitcoins.

Para que un bloque sea generado cada diez minutos, el protocolo actualiza cada dos semanas la dificultad del problema que todos los nodos generadores están intentando resolver, ajustándola al poder computacional de toda la red.

Debido a los incrementos en la dificultad para obtener bitcoins por medio de la minería, ya hace mucho tiempo que ésta dejó de estar al alcance del usuario común de una PC. Hoy en día, la mayoría de los usuarios de Bitcoin obtienen sus cripto-monedas a cambio de los productos que venden, o en sitios de *trading*, o bien en transacciones cara a cara con mineros u operadores que compran bitcoins y los venden cobrando una comisión.

Tarifa de transacción

Debido a que los nodos no tienen la obligación de incluir transacciones en los bloques que generan, los remitentes de bitcoins pueden pagar voluntariamente una tarifa de transacción. Al hacerlo, además de acelerar la transacción, proveen incentivos a los usuarios que mantienen nodos generadores (vale decir, a los mineros). Los nodos generadores retienen el valor correspondiente a las tarifas de todas las transacciones incluidas en los bloques que han resuelto.

Dichas tarifas – cuando se pagan – suelen ser una fracción insignificante del monto enviado, si se las compara con las de cualquier otro sistema de transferencia de valor. Por ejemplo, si decidimos enviar 100 bitcoins puede

que el software nos sugiera pagar una tarifa de 0,005 bitcoins.

Las tarifas de transacción irán cobrando más importancia cuanto más bajo sea el premio por bloque. En el futuro, los mineros se verán motivados a mantener los nodos generadores por la suma de pagos en concepto de tarifas que puedan acumular, más que por los bitcoins que sean capaces de generar.

Peculiaridades monetarias

A diferencia del dinero de curso forzoso, Bitcoin no puede ser controlado por ninguna autoridad debido a su naturaleza descentralizada. La expansión de la base monetaria está predeterminada por el software de Bitcoin y es conocida por todos, de modo que no es posible afectar el poder adquisitivo de los usuarios manipulando la cantidad de bitcoins en circulación.

Bitcoin es un medio de pago irreversible. Las transferencias son realizadas directamente entre los nodos, sin un procesamiento centralizado por un tercero, lo cual hace imposible tanto la reversión involuntaria de pagos como la cancelación de transacciones mutuamente acordadas.

Así, el envío de bitcoins se asemeja, en los beneficios y en los riesgos que supone, al envío de dinero en efectivo. No obstante, muchos sitios ofrecen servicios similares a *e-bay* o *Mercado Libre* para facilitar el intercambio de bienes y servicios por bitcoins (por ejemplo, promoviendo la calificación entre los usuarios y/o reteniendo los fondos hasta que las partes expresan conformidad).

El software de Bitcoin (también denominado “**cliente Bitcoin**”) que los usuarios tienen instalado en sus ordenadores transmite cada transacción a los nodos cercanos, que a su vez la propagan a toda la red. Las transacciones inválidas son rechazadas por los clientes honestos (aquellos que se atienen al protocolo de la cadena de bloques en uso). Por el momento, la mayoría de las transacciones pueden realizarse gratuitamente, pero ya hemos visto que es posible pagar una tarifa para que los mineros prioricen (aceleren) su procesamiento.

El número total de bitcoins tenderá a 21 millones con el tiempo. Su oferta crece en una serie geométrica (con una razón constante); así, en 2013 la mitad

de la oferta total habrá sido generada, y en 2017, 3/4 de la misma. A medida que la cantidad de bitcoins se aproxime al límite de 21 millones, se espera que la economía Bitcoin entre en deflación, esto es, que el poder adquisitivo de cada bitcoin aumente, probablemente hasta alcanzar cierta estabilidad.

Los bitcoins, entre tanto, son divisibles hasta ocho decimales (dándonos 2,1 x 10^{15} – vale decir 2,1 cuatrillones – de unidades totales), y potencialmente aún más de ocho decimales, lo cual remueve las limitaciones prácticas a los ajustes de precio en un contexto deflacionario.

La economía Bitcoin es aún pequeña si la comparamos con otras economías ya establecidas, y el *software* todavía se encuentra en estado *beta*. Sin embargo, todo tipo de bienes y servicios, desde automóviles a trabajos de programación *freelance*, están en este momento siendo intercambiados por bitcoins. Además, hay gran cantidad de sitios web que facilitan el intercambio de todo tipo de divisas por bitcoins, y admiten diversos sistemas para transferir los fondos.

¿En qué resultará?

Un posible escenario de fracaso para Bitcoin es el de una campaña gubernamental global en contra del software y de los sitios que aceptan bitcoins. Pero dada la naturaleza del sistema, la eliminación total de Bitcoin (así como de cualquier otra red P2P) no parece tecnológica ni económicamente viable.

Nadie sabe con certeza cuál será el destino de Bitcoin; todo lo que sabemos es que la idea de una cripto-moneda descentralizada llegó para quedarse.

Por qué nos cuesta entender el funcionamiento de Bitcoin

Incluso los más preparados entre nosotros parecen requerir al menos dos o tres explicaciones antes de comprender efectivamente cómo es que funciona Bitcoin. Esto se debe a que **Bitcoin desafía una serie de conceptos rara vez cuestionados**, que es necesario desaprender si se han de incorporar otros mejores.

El esfuerzo, por lo tanto, es doble. Así como la teoría de la universalidad de los "cuatro elementos" (aire, agua, fuego, tierra) entorpeció durante siglos el progreso científico, la teoría cuantitativa del dinero – y su correlato de un sistema monetario dirigido por "especialistas", con un banco de bancos en su centro – ha tenido un efecto mental devastador sobre generaciones enteras de legos y estudiosos.

El problema es que aún sabiendo por qué Bitcoin es superior a cualquier otro sistema monetario, muchos tienden a preferir lo ya conocido con tal de no incursionar en territorios inexplorados. La eterna batalla entre el conservador – partidario de lo malo conocido – y el aventurero – partidario de lo bueno por conocer – se libra en realidad en el pecho de cada ser humano. Pero una vez rechazado el legado de ideas falsas y **vencida la inercia de las costumbres, el camino se hace cuesta abajo** para el aventurero – quien le abrirá paso también al conservador.

¿Cuáles son esas costumbres tan arraigadas que hacen aparecer a Bitcoin como algo inverosímil?

• **Estamos habituados a que el acto de pagar esté separado del acto de registrar el pago.** En rigor, por medio de Bitcoin nadie paga (nadie envía ni recibe bitcoins). Lo que hace la gente es modificar saldos en una suerte de libro contable descentralizado. Así pues, el acto de pagar se confunde con el de registrar el pago.

• **Estamos habituados a pensar que el sistema monetario necesita ser custodiado por una casta privilegiada.** El protocolo de Bitcoin no protege a alguien o a algún grupo en particular, sino a la herramienta misma – y así a todos los que la usan.

• **Estamos habituados a que nuestras cuentas bancarias estén asociadas a nuestra identidad.** Las direcciones Bitcoin son anónimas si así lo desean sus dueños.

• **Estamos habituados a que el movimiento de fondos sea conocido sólo por quienes están directamente involucrados en una transacción (las partes y el tercero que procesa el pago).** En Bitcoin la información acerca de todas las transacciones es pública y de fácil acceso.

• **Estamos habituados al dinero como recibo con más o menos respaldo.**

En el caso de Bitcoin, unidad y recibo son una misma “cosa” imposible de replicar o falsificar.

II – Las Ventajas

Por qué Bitcoin es superior a otras monedas

La respuesta rápida: porque nadie – ningún comité de "expertos" – controla su destino, y porque las reglas que fija el protocolo ideado por Satoshi Nakamoto no se imponen; cada usuario elige aceptarlas. Ahora bien, ¿qué significa esto, en la práctica, para el usuario?

Repasemos las ventajas de Bitcoin…

- Mayor privacidad, al eliminar la interferencia de terceros en las transacciones.
- Aumento decreciente y predecible de la masa monetaria, lo cual ayuda a preservar – y probablemente a mejorar – el poder adquisitivo de los usuarios.
- Menores – e incluso nulos – costos de transacción en la web, cuyos niveles actuales – por ejemplo a través de *PayPal* – entorpecen el libre intercambio.
- Simplifica y acelera el pago de persona a persona, prescindiendo de intermediarios no deseados.
- Una dirección Bitcoin puede ser anónima, si así lo desea el usuario.
- Permite hacer transferencias a cualquier parte, ignorando barreras geográficas y políticas.
- Es transparente: aunque nadie está forzado a revelar su identidad, todas las transacciones quedan grabadas en un registro de libre acceso.
- Admite transacciones complejas (depósitos en custodia; seguros de depósitos; garantías; mediación, etc.) con un firme respaldo criptográfico para todo tipo de reglas y condiciones libremente

acordadas por las partes.

- Nunca se detiene: no hay feriados ni fines de semana para las operaciones en bitcoins.
- Hace viables los micropagos a gran escala.
- Impide la congelación de fondos.
- Impide la reversión involuntaria de pagos.
- Impide la restricción arbitraria de bienes y servicios que pueden adquirirse.
- Permite la acumulación de fortunas enormes en un espacio ínfimo.
- Puede ocultarse fácil y gratuitamente – sin tener que apelar a terceros para su resguardo y traslado.
- Se puede guardar en múltiples localizaciones simultáneamente.
- No requiere confianza en un tercero ni en un determinado sistema legal para preservar su valor.
- Facilita la protección contra el robo en todas sus formas – impuestos inclusive: la tecnología en la que se basa el protocolo de Bitcoin es varias veces más segura que la empleada por los bancos y las tarjetas de crédito.
- No puede ser eliminado por ataques legales/informáticos, dada su naturaleza descentralizada.
- No puede falsificarse.
- Es fácil e instantáneamente reconocible.
- Es, a los fines prácticos, infinitamente divisible.

Por unas pocas razones que hoy ya todos admiten, el e-mail ha reemplazado al correo postal en sus funciones principales… ¿cuántas razones a favor de

Bitcoin tienen que acumularse para que el dinero de curso forzoso pase a la historia?

EN POCAS PALABRAS…

Estas son las frases que fueron publicadas en el foro de Bitcoin en respuesta a la siguiente consigna: defina Bitcoin para los no iniciados, en pocas palabras.

"Bitcoin es la manera de intercambiar valor más costo–efectiva."

"Bitcoin es dinero en efectivo móvil para el ciudadano del mundo – Bitcoin no tiene fronteras."

"Bitcoin es la red informática más potente del mundo."

"Bitcoin es más difícil de hackear que cualquier banco."

"Bitcoin le hará a los grandes bancos lo que el e-mail le ha hecho al Servicio Postal, y lo que bittorrent le ha hecho al copyright."

"Bitcoin les hará a los ejecutivos bancarios lo que Internet le ha hecho a los agentes de viajes."

"Bitcoin será la mayor oportunidad para la innovación que ha visto el mundo desde la revolución industrial."

"Cualquier persona en cualquier país puede enviar y recibir bitcoins sin tener que pedir autorización, ni abrir una cuenta ni firmar papeles."

"Bitcoin = cuentas bancarias en Suiza para el común de la gente."

"Utilice hoy el medio de intercambio del mañana."

"Bitcoin: porque usted es el dueño de su dinero."

CÓMO EXPLICARLE A TU ABUELA EL FUNCIONAMIENTO DE BITCOIN

Lasse Birk Olesen, fundador de BitcoinNordic.com, ha encontrado una manera eficaz de explicar el funcionamiento de Bitcoin en pocas palabras.

Antes que él, miles de *nerds* – acostumbrados como estaban a hablar sólo entre ellos – habían fracasado en el intento de sintetizar, para el común de la gente, las propiedades de la nueva moneda digital. Ahora, gracias a Olesen, todo lo que tu abuela necesita saber acerca de Bitcoin puede encontrarlo en un único párrafo:

"¿Cómo funciona Bitcoin? Imagine un tipo especial de email que no puede ser copiado. Esto significa que cuando usted lo envía a otra persona, éste email automáticamente se borra de su propia casilla de correo electrónico (el destinatario pasa a tener el email que usted ya no tiene). Ahora también imagine que sólo existe una cantidad finita de estos emails especiales, y que nadie puede crear más de los que ya existen. Debido a estas propiedades, la gente ha comenzado a considerar a estos emails como algo valioso. Estos emails especiales, por supuesto, se llaman bitcoins."

No es, por cierto, una explicación completa ni muy rigurosa, pero tu abuela sabrá apreciarla. Después de todo, a ella no le hizo falta entender los pormenores técnicos de una red P2P antes de animarse a usar el correo electrónico. Y francamente, a nosotros tampoco.

14 cosas que se pueden hacer con Bitcoin que de otro modo no se podrían hacer

1. Donar 10 centavos a tu blogger favorito con un costo de transacción menor a un centavo.

2. Escribir un libro, crear una obra de arte, tocar y/o cantar una canción; subirlos a Internet y venderlos sin demoras. Sin necesidad de carros de compras, editores ni distribuidores; sin tener que recurrir a PayPal o a las tarjetas de crédito.

3. Enviar 1 dólar a una persona con un costo de transacción menor a un centavo, sin importar la distancia a la que ésta se encuentre.

4. Enviar diez mil dólares a una persona con un costo de transacción menor a un centavo, sin importar la distancia a la que ésta se encuentre.

5. Tener una cuenta de ahorro sin necesidad de pagarle a un tercero por el

servicio.

6. Cobrar instantáneamente todo el dinero ganado en un casino *online*. Poder hacerlo sin dar a conocer nombre o domicilio.
7. Reunirse con amigos a jugar al póker sin tener que pasar previamente por un cajero automático para retirar efectivo. Saldar las cuentas al final de la noche sin necesidad de conseguir cambio.
8. Salir a comer con amigos sin tener que pedirle al mozo que haga las cuentas por separado. Puede pagar uno por todos y luego cobrarles exactamente lo que cada uno debe, hasta el último centavo, sin necesidad de llevar efectivo.
9. Comprar el almuerzo para tus compañeros de trabajo sin necesidad de juntar previamente el dinero. En cuanto les hayas enviado tu dirección de pago, cada uno podrá pagarte lo que le corresponde sin moverse de su escritorio.
10. Abrir una tienda *online* en minutos sin tener que utilizar carros de compras ni procesadores de pagos, y sin costos adicionales.
11. Cobrar por un bien o servicio sin tener que preocuparte porque PayPal o las empresas de tarjetas de crédito te pidan que les devuelvas el dinero. Con Bitcoin, todos los pagos son definitivos; no pueden revertirse.
12. Donar dinero a una organización que tu gobierno (o Pay Pal) desaprueba; poder hacerlo anónimamente.
13. Proteger tu riqueza de la inestabilidad económica y las políticas financieras absurdas de tu país sin destruir el medio ambiente.
14. Viajar a otro país y poder costear tus gastos sin necesidad de pasar por una casa de cambio (en un futuro cercano).

Un problema fundamental, solucionado

La implementación del protocolo Bitcoin resuelve el siguiente problema: "cómo aprovechar todas las cualidades de la mejor moneda concebible… sin la necesidad de confiar en nadie". Increíble, ¿no?

En los sistemas monetarios vigentes, basados en dinero de curso forzoso, los usuarios no tienen más remedio que "confiar" en la buena voluntad de toda clase de personas – funcionarios públicos, banqueros, personal administrativo, etc. Los usuarios de este tipo de dinero son auténticos rehenes, y por tal motivo su confianza es y será, inexorablemente, víctima de abusos.

Con Bitcoin, en cambio, ninguna persona está en condiciones de manipular el sistema con el fin de abusar del prójimo: nadie puede imprimir más dinero; nadie puede volver a utilizar ni falsificar las monedas; y nadie puede disponer de las monedas de otra persona sin tener acceso directo a sus claves privadas.

Cuando alguien intenta infringir las "reglas" de Bitcoin modificando su protocolo, genera en el acto un sistema paralelo, totalmente distinto e incompatible (cuyas "monedas" no serán reconocidas por los usuarios de Bitcoin).

De modo que Bitcoin seguirá funcionando mientras haya usuarios que respeten las reglas inscritas en su protocolo – y los incentivos para hacerlo son cada vez más poderosos.*

** Aclaración: uno adhiere a las reglas del protocolo Bitcoin simplemente ejecutando el software de Bitcoin.*

El sentido de la minería

No es posible exagerar la importancia de la minería en el sistema ideado por Satoshi Nakamoto. Demos un paso atrás y admiremos el esplendor de la organización espontánea, gracias a esta breve explicación de Paul Bohm (ver el escrito original, en inglés):

"Para asegurarse de que a un atacante le sea más caro adquirir el poder computacional necesario para poder engañar al sistema, Bitcoin cuenta con una estructura de incentivos. Los usuarios que aportan poder computacional (los "mineros") se ven recompensados por su trabajo; así, cuando el valor del bitcoin aumenta y por lo tanto atacar al sistema se torna más rentable, también se torna más rentable para los usuarios honestos añadir recursos computacionales a la red.

En cualquier momento dado, los mineros invierten en equipos tanto como es rentable para cada uno de ellos. La "minería" no es en absoluto un desperdicio de energía, sino todo lo contrario: es una forma increíblemente eficiente de hacer que los ataques no sean rentables.

Bitcoin incentiva a los mineros a fin de proteger el consenso que se da entre los nodos de la red, pero nunca utiliza más recursos computacionales de los que necesita para proteger su integridad y buen funcionamiento."

La naturaleza de Bitcoin

Como ilustran los ejemplos de *BitTorrent* y *Skype* – entre muchos otros protocolos de redes *peer to peer* – las buenas ideas, en Internet, se transmiten vertiginosamente. Así pues, la expansión viral de Bitcoin puede ocurrir en cualquier momento.

Cabe entonces imaginar un futuro en el cual millones de personas utilizan Bitcoin regularmente. Aún bajo presión gubernamental, Bitcoin podría evolucionar como una suerte de sociedad paralela, cohesionada por un sinfín de acuerdos plenamente voluntarios. Los usuarios de Bitcoin podrían contactarse para negociar al margen de regulaciones absurdas; para armar y financiar emprendimientos difíciles de gravar; para solicitar y ofrecer alojamiento en todas partes del mundo; para ayudar a las víctimas de regímenes opresivos; etc. etc.

Bitcoin no es una compañía – como algunos distraídos han supuesto. Tampoco es "simplemente una herramienta". Bitcoin es, en todo caso, un marco para el desarrollo de herramientas. Por su capacidad para absorber constantemente innovaciones sin abandonar su esencia, Bitcoin se parece más bien a Internet – se confunde con Internet… y vivirá tanto como Internet.

La moneda universal

Gracias a la posibilidad de intercambiar bitcoins por – hasta la fecha – más de noventa signos monetarios, Bitcoin podría acabar convirtiéndose en el método de elección para la transferencia internacional de fondos. En tal caso, los habitantes de países del "tercer mundo" serían los más beneficiados.

¿Ganará Bitcoin tracción en el tercer mundo, antes que en el primero? Las condiciones para ello están dadas: bajo grado de bancarización; regulaciones asfixiantes; extensa economía informal; alta inflación; ciclo económico frecuente; comisiones abusivas por servicios de remesas; explosión en la venta de móviles…

De cualquier manera, las ventajas de Bitcoin no pasarán desapercibidas por mucho más tiempo, en el tercero ni en el primer mundo.

Hoy en día, ***mail*** es sinónimo de ***e-mail***; ¿será “moneda”, en un futuro no lejano, sinónimo de Bitcoin?

El sistema monetario más seguro

Quien crea que los algoritmos criptográficos empleados por Bitcoin – SHA256 y ECDSA – no son lo suficientemente confiables, tampoco debería confiar en las tarjetas de crédito, ni en cualquier tipo de transferencia bancaria electrónica.

¿Y no podrían las computadoras del futuro burlar la seguridad que ofrece hoy Bitcoin?

Quizás. Pero recuerda: de ser necesario, el software puede actualizarse (de hecho, se actualiza periódicamente). El mismo problema enfrentarían instituciones financieras tales como los bancos, que también dependen de la criptografía para efectuar transacciones.

Eventualmente, las nuevas tecnologías podrían incluso desafiar el rol monetario de la plata y el oro, al acabar de alguna manera con su relativa escasez (minería en asteroides; extracción a partir de arenas o de agua marina) – con un agravante: las cualidades físicas de los metales preciosos no pueden ser actualizadas.

En cambio, ninguna tecnología podrá jamás alterar los axiomas de la matemática, lo cual garantiza que el número total de bitcoins nunca será incrementado en forma discrecional.

Ahora bien… ¿pueden perderse los bitcoins? Claro que sí, del mismo modo que pueden perderse billetes, lingotes u otras pertenencias. Pero también

pueden mantenerse adecuadamente resguardados *(ver más adelante "Cómo crear una "caja fuerte" de bitcoins en sólo 4 pasos")*.

¿Puede fracasar Bitcoin?

Un escenario que podría suponer el fracaso de Bitcoin es el de una prohibición total y mancomunada por parte de los gobiernos más poderosos del planeta.

¿Pero qué puede hacer un Estado frente a Bitcoin?… en realidad, lo mismo que frente a *BitTorrent* o a *Wikileaks*: nada que funcione. Irónicamente, los ataques gubernamentales podrían incluso fortalecer a Bitcoin.

Eso mismo le ocurrió a los sistemas descentralizados para el intercambio de archivos de música: florecieron luego de la desaparición forzada de *Napster*, y prosperaron al calor de la persecución.

Cuando se trata de software de código abierto, lo que no se mata no sólo se hace más fuerte; también se multiplica, y se propaga, y se hace más confiable, más rápido, más amigable, etc. etc.

Un sistema indestructible

Para frenar a Bitcoin hay que eliminar internet. Punto. Es la única manera de lograr que todas y cada una de las computadoras que ejecutan el software de Bitcoin queden (al menos transitoriamente) incomunicadas.

¿Y una catástrofe a gran escala no acabaría con Bitcoin? No necesariamente: basta que una sola de dichas computadoras no sea destruida en el proceso para que – una vez restablecidas las conexiones – los legítimos dueños de las criptomonedas digitales puedan volver a operar con normalidad.

Cabe recordar que las claves privadas (aquellas que garantizan la posesión de un determinado número de bitcoins) se encuentran en poder de los usuarios, quienes pueden conservarlas en sus discos rígidos, pero también en cualquier otro soporte de información, incluyendo papel.

El eslabón más débil de Bitcoin no es el protocolo creado por Satoshi

Nakamoto (el cual, justamente, asegura el funcionamiento descentralizado del sistema), sino los grandes sitios de intercambio en Internet. Pero si bien los ataques reiterados a este tipo de sitios podrían llegar a minar la confianza en el sistema, también podrían incentivar el uso de otras vías de intercambio, favoreciendo así la descentralización.

Y una vez que los puntos de intercambio están lo suficientemente descentralizados… ¿cómo frenar la compra y venta de bitcoins?

Enfrentémoslo: el Estado seguirá aferrándose a lo que todavía puede controlar – aunque eso que puede controlar sea cada vez menos relevante.

¿O es que el Estado realmente no controla nada, y sólo ahora estamos empezando a entenderlo?

Atendamos ahora a las fortalezas de Bitcoin como sistema de incentivos. Para destacarlas, tomaremos como referencia el ejemplo de otro proyecto – enormemente exitoso, por cierto – que también está basado en una red *peer to peer*: BitTorrent.

• **BitTorrent:** quienes lo utilizan tienen que lidiar con archivos "pesados" (entra en consideración el tiempo, el almacenamiento y, en ocasiones, el ancho de banda).

» **Bitcoin:** los datos requeridos para autorizar cada transacción se transmiten instantáneamente y ocupan un espacio despreciable.

• **BitTorrent:** demanda el aporte de muchos usuarios (no necesariamente remunerados) para asegurar la integridad de cada archivo.

» **Bitcoin:** el aporte de un único usuario es suficiente para concretar una transacción, y los mineros (quienes confirman las transacciones) son remunerados por su trabajo.

• **BitTorrent:** es utilizado en general para satisfacer necesidades secundarias.

» **Bitcoin:** permite la transferencia de unidades de valor arduamente obtenidas por los usuarios.

• **BitTorrent:** es relativamente fácil sustituir el servicio que brinda (por

ejemplo, pagando una módica suma por los contenidos buscados).

» **Bitcoin:** las alternativas disponibles (PayPal, Western Union, sistema bancario) se parecen tanto a Bitcoin como un carro tirado por bueyes a un avión supersónico.

Dicho esto, cabe recordar que BitTorrent no sólo ha resistido los embates de las corporaciones y los gobiernos más poderosos que existen, sino que sigue creciendo a buen ritmo y ganando adeptos en todo el mundo. Según puede leerse en Wikipedia, en Enero de 2012 el número total de usuarios mensuales de BitTorrent era mayor a 250 millones, y en cualquier instante BitTorrent tiene, en promedio, más usuarios activos que YouTube y Facebook juntos.

La cuestión del anonimato

Algunos criptógrafos de la línea más dura opinan que Bitcoin en realidad no preserva totalmente el anonimato de los usuarios, y que éste es un evidente punto débil del sistema. Lo cierto es que usando Bitcoin uno puede mantener el nivel de anonimato que desea, pero la inmensa mayoría de los usuarios no necesitan mantenerse 100% anónimos todo el tiempo y frente a todo el mundo; les basta con poder elegir ante quién revelar su identidad, y en relación a qué direcciones Bitcoin.

Pero – insisten los criptógrafos ***hardcore*** – la identidad de un usuario de Bitcoin podría llegar a asociarse a una determinada dirección Bitcoin, si se descubre la dirección IP desde la cual el usuario ha operado. A lo cual nosotros respondemos: una dirección IP no tiene por qué llevar nuestro nombre, y aún si lo llevara consigo, eso no sería suficiente para involucrarnos en una determinada transacción: otro podría estar usando la dirección que se ha generado en nuestra computadora; otro podría haber usado las llaves privadas que alguna vez estuvieron en nuestro poder; otro podría haber utilizado nuestra computadora de manera presencial o remota…

Por otra parte, si un usuario de Bitcoin quiere hacer una transacción sin dejar huellas, puede hacerlo generando una dirección Bitcoin en una computadora ajena, o bien desde una billetera web, sin contar con conocimientos técnicos excepcionales.

Claro – dicen a coro los criptógrafos, mientras se acomodan los anteojos –, pero con suficiente interés, dedicación y recursos, podríamos llegar a presumir, con un alto grado de certeza, que tal persona fue parte de tal transacción. Concedido, pero aún la certeza más absoluta respecto a la identidad de un usuario no alcanzará para congelar los fondos ligados a una dirección Bitcoin – ¡ni siquiera para saber si el individuo que fue identificado tiene acceso a esos fondos!

Bitcoin está diseñado para que el dueño de una determinada cantidad de bitcoins sea el único autorizado a disponer de esos bitcoins. Ahora bien, que hayamos poseído una determinada cantidad de bitcoins no significa que sigamos necesariamente en posesión de los mismos: podríamos haber perdido nuestra billetera (nuestra llave privada), o bien olvidado la contraseña para acceder a esos bitcoins, o bien esos bitcoins podrían haber llegado a nuestra dirección sin nuestro conocimiento, o bien podríamos haberlos transferido a alguien cuya identidad no conocemos.

Como la identidad de los usuarios de Bitcoin no se encuentra irremediablemente ligada a cuenta o transacción alguna, todo esfuerzo por averiguarla chocará, tarde o temprano, con una negativa plausible. Esta posibilidad, especialmente apreciada por las víctimas de regímenes opresivos, no la ofrece ninguna otra forma de dinero electrónico.

En conclusión: tras invertir grandes cantidades de recursos tecnológicos y humanos, a lo sumo será posible probar que alguien que no desea revelar su identidad tuvo quizás, alguna vez, bitcoins bajo su control, sin saber siquiera cuántas otras direcciones Bitcoin posee (es posible generar una dirección Bitcoin por cada transacción), ni si aún los posee, ni si los ha transferido a otra persona o simplemente a otra de sus direcciones, ni si alguien más – y de qué manera – es capaz de transferirlos… y sin poder congelar ni confiscar esos fondos, ni decidir a qué fines pueden ser destinados.

Bitcoin impide los abusos de poder que son perpetrados de una manera extraordinariamente sencilla y económica por medio del sistema bancario semi-estatal. Y nada puede hacerse para eliminar a Bitcoin, ya que su funcionamiento depende de la propia infraestructura de telecomunicaciones que hace posible Internet. Por eso, desde el punto de vista de una institución con el poder de esclavizarnos a través del sistema monetario, Bitcoin es como un virus informático que no puede ser eliminado sin destruir todo el sistema.

LA EXPANSIÓN DE LA BUENA MONEDA

Así como la física sirve para explicar el movimiento de la carreta, del automóvil o del avión, la ciencia monetaria sirve para explicar el funcionamiento de la sal, del oro o de Bitcoin como medios de intercambio y preservación del valor. Desde la carreta hasta el avión, y desde la sal hasta Bitcoin, **lo que ha cambiado no son las leyes mismas que gobiernan la realidad, sino la manera de aprovecharlas**. Las leyes básicas de la economía son tan inmutables como las de la física, y mantendrán su validez mientras los seres humanos tengan necesidades que satisfacer – esto es: mientras existan seres humanos.

No fue un milagro – ni siquiera una novedad tecnológica, sino una nueva aplicación de la tecnología existente para manipular los metales – lo que hace miles de años hizo posible la monetización del oro y la plata.

Fast forward hasta el año 2009: una nueva aplicación de tecnologías ya disponibles (el software moderno, por caso, lleva entre nosotros unos cincuenta años) hace posible la creación de la primera moneda electrónica descentralizada. **Las herramientas estaban ahí; sólo faltaba un Satoshi Nakamoto**.

Hay dos razones por las cuales Satoshi eligió, para Bitcoin, el modelo de los metales preciosos. La primera es empírica: éste funcionó durante miles de años. La segunda, lógica: funcionó porque los metales preciosos, en particular el oro, cumplen con todos los requisitos de la buena moneda: durabilidad, portabilidad, fácil almacenamiento, difícil falsificación, homogeneidad, divisibilidad, fungibilidad, amplia distribución geográfica y, sobre todo, baja proporción entre su producción anual y el stock de existencias.

Ahora bien, si la aceptación del oro – tan amplia en el espacio como prolongada en el tiempo – es consecuencia de sus peculiares atributos, y Bitcoin es, objetivamente, mejor moneda que el oro, hemos de concluir que el uso de Bitcoin continuará expandiéndose. Y, como se ha visto en el caso de los metales preciosos, **toda la violencia del mundo es incapaz de frenar la expansión de la buena moneda**.

LA BUENA MONEDA EN LA ERA DE INTERNET

Ni el tiempo, ni la geografía, ni la fuerza bruta son obstáculos para la expansión de la buena moneda. Y si no lo fueron durante miles de años, menos aún lo serán ahora.

Veamos algunos ejemplos:

Algunas de las primeras monedas tenían una composición muy estable, como es el caso de la redonda moneda china, "qian", de cobre, aparecida en el siglo IV a.C. y que se mantuvo como moneda oficial durante dos mil años.

(...)

Las monedas "qian" de bronce o cobre que habían sido limadas para beneficio del gobierno de turno eran, de hecho, dinero de baja calidad, fiduciario, cuyo valor dependía del número de monedas de oro o cobre de buena calidad por las que se podían intercambiar.

(...)

Las monedas de oro y plata solían circular fuera del país que las emitía dado su valor intrínseco; así, el peso de plata español, cuyo material provenía de las minas del Perú y de México, se convirtió en una moneda de uso corriente en China a partir del siglo XVI.

(Ver artículo completo en Wikipedia)

Regresemos a nuestro siglo XXI. G**racias a la comunicación instantánea y de alcance global, ninguna herramienta útil pasa desapercibida para el común de la gente**. Cientos de millones de personas que tan sólo unos años atrás no se atrevían a operar una casilla de email, hoy utilizan cotidianamente Facebook, Twitter y Skype. Imaginen la manera en que puede llegar a propagarse una herramienta que sirve para resguardar el fruto del propio trabajo (para muchos una cuestión de supervivencia).

El dinero de curso forzoso es incapaz de preservar el valor. De hecho, cabe argumentar que ese es, precisamente, el motivo por el cual nos obligan a usarlo. En todo caso, no tenemos alternativa: al igual que el mafioso cuando nos advierte que tenemos que pagarle protección "porque estamos en un barrio peligroso", el gobierno nos recuerda constantemente que sin su protección

quedaríamos a merced de los cuatro jinetes del apocalipsis - y la expresión "no, gracias" no figura en su diccionario.

Quienes desde el poder usan sistemáticamente la fuerza bruta tienen la costumbre de hacerlo bajo la excusa de que están velando por nuestros intereses. No pueden decirnos en la cara que nos van a imponer el mal dinero, puesto que nos reiríamos y simplemente los ignoraríamos, como a un hombre disfrazado de Napoleón que nos exhorta a obedecer sus órdenes. Si un gobierno pretende controlar el sistema monetario, primero tiene que asegurarnos que el buen dinero (el dinero que libremente hemos elegido usar) será el respaldo del nuevo signo monetario. Recién cuando nos acostumbremos a usar éste en lugar de aquél podrán decirnos que el dinero que habíamos elegido libremente no era más que una "bárbara reliquia", que en la esfera monetaria no puede haber competencia, y que el único "respaldo" que vale es, en realidad, la fuerza.

Pero no toda la población productiva cae en esta vieja trampa. Si algo nos han enseñado miles de años de historia es que la presión ejercida sobre la capacidad de ahorro no es gratuita: **cuanto mayor sea el hostigamiento, más alto cotizará el refugio de valor, y más enérgicamente será defendido**. Todo lo que puede hacerse desde el Estado es hundir a la buena moneda en el mercado negro hasta el colapso del sistema monetario. Luego no quedará otra opción más que levantar las restricciones y dejar que la buena moneda vuelva a circular más o menos libremente.

Lo que ningún erudito pudo anticipar es que este fraude cíclico iba a toparse algún día con un obstáculo infranqueable: con una moneda digital y universal que nadie puede controlar ni eliminar, capaz de circular a salvo de las arbitrariedades de los poderes de turno.

Curiosamente, **nadie vio venir a Bitcoin**. Y decimos "curiosamente" porque el siglo XXI será recordado como el siglo de Bitcoin.

¿Es necesario el visto bueno del Estado?

Los bitcoiners están divididos en cuanto al significado y las posibles consecuencias del reconocimiento oficial de Bitcoin.

Por un lado, **hay quienes insisten en que, para ser ampliamente aceptado, Bitcoin debe presentarse como una simple alternativa a PayPal. Según ellos, “legitimidad” es sinónimo de bendición gubernamental**, por eso instan a todo negocio relacionado con Bitcoin a registrarse ante funcionarios que ni siquiera han oído hablar de Bitcoin; a cumplir con regulaciones elaboradas específicamente para obstaculizar la innovación; a invertir en abogados y contadores incluso antes de saber si el negocio es rentable; a demostrar su inocencia (antes de haber siquiera actuado) frente a una autoridad arbitraria, corrupta, violenta e ignorante. (Lo cierto es que ningún emprendimiento verdaderamente innovador alcanza el éxito en Internet mediante una licencia gubernamental – es decir mediante un permiso otorgado por una organización cuyo negocio es el de entorpecer el libre intercambio).

Otros, en cambio, saben perfectamente que – tarde o temprano – los privilegiados por el actual sistema monetario verán a Bitcoin como una amenaza para sus intereses, y que harán todo lo posible para demonizarlo (luego de corroborar que no pueden eliminarlo). Estos otros bitcoiners han comprendido que la gente se acerca a Bitcoin precisamente buscando un refugio, una alternativa al dinero de curso forzoso, y que es inútil disimular la naturaleza de Bitcoin con el fin de apaciguar al Estado.

De todas maneras, que Bitcoin aún no haya sido reconocido oficialmente como dinero no se debe al temor de los gobiernos, ni a la falta de jurisprudencia al respecto. Se debe a que **los beneficiarios del sistema monetario vigente habitan una burbuja** inflada por intelectuales que han prostituido su intelecto. Y como dentro de esa burbuja se respira mitología, no tienen ni la más remota idea de lo que Bitcoin significa para ellos. **Están demasiado cómodos como para preguntarse cuál es el origen de su comodidad.**

El estatus legal de Bitcoin

Estos son los fragmentos más destacados de la entrevista realizada a Matt Hutchins, el primer abogado especializado en Bitcoin, en el episodio 44 de The Bitcoin Show, el 8 de Septiembre de 2011:

The Bitcoin Show: *Las implicancias legales de Bitcoin son tan complejas y fascinantes como sus aspectos técnicos – aunque de maneras muy diferentes: uno es extremadamente lógico y el otro es extremadamente…*

legal [risas].

Matt Hutchins: *Bueno, digamos que el aspecto legal tiene su propia lógica. Yo siento una gran admiración por Gavin y todo su equipo técnico; están haciendo un gran aporte a toda la comunidad… en realidad a Internet como un todo, al desarrollar esta tecnología que llamamos Bitcoin. Toda nueva tecnología tiene implicancias legales. No vine aquí a hablar de aplicaciones particulares de leyes vigentes a Bitcoin, sino más bien a explicar por qué algunas personas deberían pensar en estos asuntos legales desde la perspectiva del derecho, y considerar la asesoría legal.*

TBS: *Nos falta saber muchas cosas al respecto. (...) Tenemos leyes antiguas que no pueden aplicarse fácilmente a las nuevas tecnologías, más aún a algo tan revolucionario como Bitcoin.*

MH: *(...) Cuando tratamos con preguntas legales, tenemos que tener en cuenta todas las posibles respuestas, y pensar detenidamente en todas las palabras que vamos a emplear; en cómo pueden ser interpretadas. ¿Qué perspectiva puede preponderar?; ¿qué perspectiva puede servir a mis intereses?… ¿cuál será más probablemente adoptada por alguna de las partes? – como ser un fiscal, o un ente regulador. No podemos ignorar eso.*

TBS: *Un mismo término puede tener un significado muy diferente en la calle y en una corte. Así que por ejemplo Bitcoin puede ser definido por mucha gente como dinero virtual, pero ¿es dinero?; ¿es virtual? Que en bitcoin.org digan que Bitcoin es dinero no significa que encaja en la definición legal de dinero. E incluso desde el punto de vista legal puede haber divergencias entre estados, países, etc.*

MH: *Así es. Si nos fijamos en el caso de la corte francesa – que tanto interés ha generado en la comunidad Bitcoin – uno de los aspectos en discusión es si Bitcoin es o no es dinero. Porque si es considerado dinero, cae bajo un cierto régimen de regulaciones, pero si es meramente una forma intangible de propiedad, entonces se le aplicarán otro tipo de regulaciones.*

Como reserva de valor uno puede en realidad utilizar cualquier cosa, siempre y cuando uno considere que aquello va a conservar el valor en el tiempo. El oro es normalmente aceptado como un medio de preservación del valor, pero como medio de intercambio en realidad no es muy práctico. De modo que, por sus semejanzas con el oro, es probable que Bitcoin tenga

también un rol importante como medio para preservar el valor. Pero en muchos sentidos puede decirse que es mejor que el oro, porque es muy fácil de transferir; es potencialmente más seguro (basta una buena contraseña para asegurar la posesión de los bitcoins); es un gran facilitador de transacciones (aunque todavía la infraestructura económica está en desarrollo, y mucha gente es reacia a gastar bitcoins justamente por su optimismo respecto al futuro del sistema).

Uno de los aspectos más importantes de la definición legal de dinero es que éste tiene que tener una identidad nacional. Bitcoin nunca ha sido utilizado como moneda nacional, pero no hay que descartar esa posibilidad: bajo ciertas circunstancias, un país podría abolir su propia moneda y adoptar a Bitcoin como moneda nacional. ¿Cómo afectaría eso al estatus legal de Bitcoin?; ¿cambiaría a partir de una decisión como esa por parte de un gobierno?

Una razón por la cual podría considerarse a Bitcoin como una forma de dinero es que existen mercados de intercambio, y por lo tanto en la práctica los bitcoins se tratan como dinero. (...)

A diferencia de la mayoría de los ***commodities*** *tangibles, los bitcoins son electrónicos, tienen un costo de transacción virtualmente nulo, son fungibles, extremadamente divisibles, y pueden intercambiarse rápidamente por gran cantidad de signos monetarios a través de internet, lo que allana la conversión entre divisas.*

TBS: *Y anula las distancias geográficas, y las fronteras políticas. Es algo tan extraordinario... Veamos, ¿de qué otras maneras puede ser definido Bitcoin?*

MH: *Hay muchas categorías en las cuales Bitcoin podría encajar, y no son todas mutuamente excluyentes. Podría caracterizarse como un título o valor. Yo creo que no es acertado porque los títulos o valores tienen un emisor institucional. En mi opinión se asemeja más a un* ***commodity****; poseer bitcoins es algo así como ser el dueño de una cantidad de carbón almacenado en un contenedor. Esa posesión es transferible. Si uno es dueño de acciones de, por ejemplo, Microsoft, el valor de lo que uno posee dependerá de las ganancias futuras de la compañía, vale decir de las decisiones que tomen sus directores, de las condiciones del mercado, etc. No*

hay ganancias futuras en términos de bitcoins; los bitcoins no generan de por sí ganancias que vayan a ser repartidas entre los dueños de bitcoins (un bitcoin hoy seguirá siendo un bitcoin en 10 años).

Respecto a Bitcoin como reserva de valor (según la típica definición legal)… Parece una definición atractiva, pero Bitcoin no involucra un contrato – en base al cual uno puede en el futuro reclamar un valor. Tener bitcoins no implica una relación con un emisor.

*Yo diría que Bitcoin es un **commodity** electrónico. Pero incluso esa definición no cierra del todo. Uno no tiene una determinada cantidad de bitcoins consigo; poseer un bitcoin equivale más bien a tener la facultad para transferir la posesión de ese bitcoin a otra persona, quien en realidad no recibe un bitcoin sino – a su vez – la facultad para transferir la posesión de ese bitcoin. Esto forma una cadena: la cadena de bloques. En otras palabras, lo único que uno posee es una llave privada que le permite firmar una transacción (transferir la posesión de bitcoins). Y es esa llave la que tiene un valor fluctuante. (...)*

III - Historia

EVENTOS DESTACADOS

Las siguientes fechas marcan los eventos más significativos en la breve y emocionante historia de esta nueva moneda digital. Como verán, todavía somos testigos de la primera infancia de Bitcoin – una etapa no apta para cardíacos.

18 de Agosto de 2008: registro del nombre del dominio "bitcoin.org".

31 de Octubre de 2008: publicación del *paper* de Bitcoin.

3 de Enero de 2009: se establece el primer bloque (*Genesis block*) a las 18:15:05 hs (GMT).

11 de Enero de 2009: lanzamiento de la versión 0.1 del cliente Bitcoin.

22 de Mayo de 2010: *laszlo* es el primer usuario en utilizar sus bitcoins para comprar una pizza. Paga BTC 10.000 (diez mil bitcoins por una pizza de US$25!).

11 de Julio de 2010: se publica en *slashdot* el lanzamiento de la versión 0.3 del cliente Bitcoin, lo cual atrae un gran flujo de nuevos usuarios.

12 de Julio de 2010: se inicia un aumento brusco (x10) del valor, que en 5 días pasa de US$0,008/BTC a US$0,08/BTC.

17 de Julio de 2010: empieza a funcionar MtGox (el primer sitio de *trading*).

6 de Noviembre de 2010: la economía de Bitcoin supera el millón de dólares. El precio en MtGox alcanza los US$0,50/BTC.

9 de Febrero de 2011: el Bitcoin alcanza la paridad con el Dólar estadounidense (1 bitcoin = 1 dólar).

14 de Febrero de 2011: se ofrece por primera vez un automóvil a cambio de bitcoins.

16 de Abril de 2011: la revista TIME publica un artículo sobre Bitcoin.

10 de Junio de 2011: el tipo de cambio hace un pico, superando los US$31, para luego caer hasta los US$10 en un lapso de cuatro días (la mayor disminución porcentual del precio hasta la fecha).

13 de Junio de 2011: el usuario del foro de Bitcoin *allinvain* anuncia que le han robado de su computadora una billetera Bitcoin con las claves privadas para acceder a BTC25.000 (veinticinco mil bitcoins, entonces equivalente a US$375.000).

19 de Junio de 2011: hackean la base de datos de MtGox y logran obtener el listado de 60.000 usuarios con sus respectivas contraseñas y direcciones de e-mail. Luego se supo que el algoritmo utilizado para proteger esa información era fácilmente vulnerable.

19 de Junio de 2011: alguien accede a una cuenta del administrador de MtGox y emite órdenes de venta por miles de bitcoins inexistentes, forzando la caída de la cotización en MtGox desde US$17,51 hasta US$0,01 por bitcoin. MtGox luego anuncia que dichas transacciones serían revertidas, y suspende las actividades durante los siguientes 7 días.

24 de Junio de 2011: la dificultad para generar bloques supera el millón con el bloque 133056.

22 de Julio de 2011: Intervex Digital lanza BitCoins Mobile, la primera aplicación relacionada con Bitcoin para iPad.

26 de Julio de 2011: Bitomat, el tercer sitio de *trading* de bitcoins (en orden de volumen transado), sufre la pérdida de 17.000 bitcoins debido a un error técnico. (En el curso del siguiente mes, MtGox adquiere Bitomat e incorpora su base de datos de usuarios; los bitcoins pagados por MtGox en esta operación son destinados al resarcimiento de los ex-usuarios de Bitomat).

29 de Julio de 2011: MyBitcoin, el primer servicio de billetera online – el primero, el más grande y el más completo – se torna inaccesible para los usuarios. Miles de personas no pueden disponer de sus bitcoins ni saben si podrán recuperarlos. Los responsables del sitio se toman una semana para informar que la seguridad del sistema había sido vulnerada por un hacker, y luego reintegran a los usuarios sólo el 49% de sus depósitos.

19/21 de Agosto de 2011: Primera Conferencia y Exposición Mundial de Bitcoin, en Nueva York, EE.UU.

17 de Noviembre de 2011: luego de meses de lento declive, el precio del bitcoin toca fondo en US$2. Se inicia una etapa de rápida recuperación, apoyada en una nueva generación de servicios que apuntan al usuario no técnico.

25 y 26 de Noviembre de 2011: Conferencia Europea de Bitcoin y Tecnología del Futuro 2011, en Praga, República Checa. Los oradores más destacados fueron: Amir Taaki, Rick Falkvinge, Max Keiser y Stefan Thomas.

7 de Diciembre de 2011: Internet Archive, el coloso de Internet dedicado a la digitalización de todo tipo de documentos, empieza a aceptar donaciones en bitcoins. Durante los primeros dos días recibe 480 bitcoins.

27 de Diciembre de 2011: el sitio regional de Nueva York de Wikimedia (la fundación que incluye entre sus proyectos a Wikipedia) empieza a aceptar donaciones en bitcoins.

15 de Enero de 2012: Bitcoin es el tema central en un episodio de la popular serie televisiva "The Good Wife".

1 de Marzo de 2012: al menos 46.000 bitcoins son robados de "billeteras calientes" (billeteras permanentemente activas que efectúan de manera automática gran cantidad de transacciones) en un hackeo a la compañía de servicios de *hosting* Linode. El sitio de *trading* Bitcoinica y el *pool* de minería Slush - los emprendimientos más afectados por el siniestro - anuncian que continuarán funcionando con normalidad. El precio del bitcoin se mantiene sin cambios significativos (en torno a los US$5).

2 de Abril de 2012: se anuncia en el foro de Bitcoin el lanzamiento de CoinDL, el iTunes del mundo Bitcoin.

30 de Junio de 2012: YCombinator, la mayor incubadora tecnológica del mundo, anuncia que está financiando Coinbase, un servicio de cartera Bitcoin *online*.

23 de Julio de 2012: WIKISPEED se convierte en el primer fabricante de automóviles en aceptar bitcoins.

16 de Noviembre de 2012: WordPress.com anuncia que empezará a aceptar bitcoins como medio de pago.

28 de Diciembre de 2012: LewRockwell, uno de los sitios libertarios más populares de la web, empieza a aceptar donaciones en bitcoins.

14 de Febrero de 2013: Reddit empieza a aceptar bitcoins como pago por su servicio premium.

17 de Febrero de 2013: Mega, el servicio de almacenamiento de archivos online de Kim Dotcom, añade a Bitcoin como medio de pago.

28 de Febrero de 2013: el precio del bitcoin supera el pico histórico de USD 31, marcando un nuevo récord.

Fases en la adopción de Bitcoin

El pasado

1. Los primeros *early adopters* se involucran en minería de bitcoins (probablemente Satoshi Nakamoto y unos pocos de sus conocidos).

2. Algunos maniáticos de las novedades tecnológicas se interesan por Bitcoin y conectan sus computadoras a la red. La dificultad para obtener bitcoins por medio de minería es tan baja que muchos acumulan cientos por día sin darles mayor importancia. Abundan los discos rígidos con abultadas billeteras que acaban descartados o formateados. Miles de bitcoins se pierden en esta etapa, pero casi nadie se lamenta por ello (aún).

3. La noticia de que existe una nueva moneda digital p2p se transmite a círculos más amplios (libertarios; militantes de la privacidad; ***geeks***). Aunque los bitcoins no pueden ser intercambiados fácilmente por otras monedas, hay quienes los intercambian por bienes digitales. La venta de bienes tangibles a cambio de bitcoins es anecdótica.

4. Un ***gamer*** descubre que hay gente dispuesta a pagar por los bitcoins que sus tarjetas de video pueden "producir". Sorprendido, se lo comenta a sus amigos. La minería con GPU rápidamente desplaza a la minería con CPU, que es mucho menos eficiente.

5. Aparecen los primeros mineros especializados. La confianza en el sistema crece y se empiezan a ensamblar máquinas dedicadas especialmente a la minería de bitcoins (*rigs*).

6. Son tantos los mineros, y es tan alta la dificultad para obtener bitcoins por medio de minería, que surgen los ***pools***. Estos distribuyen los bitcoins de acuerdo al poder computacional que aportan sus afiliados desde todas partes del mundo.

7. Muchos antiguos mineros siguen perdiendo sus bitcoins – porque ni siquiera saben que los tienen. Otros, más afortunados, descubren miles de bitcoins (ahora equivalentes a miles de dólares) en billeteras olvidadas.

8. Ya se pueden adquirir todo tipo de bienes y servicios a cambio de bitcoins. Además, los bitcoins pueden ser intercambiados por otras monedas en sitios de ***trading***.

9. Con el aumento del precio del bitcoin, algunos antiguos mineros empiezan a vender parte de sus ahorros en bitcoins, expandiendo el mercado.

10. Se multiplican los sitios de ***trading***. Los operadores ingresan al mercado e intentan sacar provecho de las fluctuaciones en la cotización. En los foros hay quienes tachan a estos individuos de "especuladores"; otros aducen que son ellos justamente los que moderan las grandes oscilaciones del precio del bitcoin.

11. El surgimiento de una gran variedad de servicios **online** para comerciantes y las mejoras al ***software*** de Bitcoin atraen a usuarios no técnicos. Aquellos usuarios que comprenden el potencial de la nueva moneda digital son todavía reacios a gastar sus bitcoins. Algunos foristas los acusan de "acaparadores"; otros los llaman "ahorristas", "inversores" y hasta "visionarios".

12. La mayoría de los medios masivos de comunicación ya se han hecho eco de la nueva moneda digital descentralizada. A pesar del escaso rigor periodístico y el tono sensacionalista que predomina en las publicaciones, Bitcoin sale favorecido: el número de usuarios aumenta con cada mención.

Plena etapa de distribución

13. Cada vez que el precio **aumenta considerablemente** se alzan voces que auguran 'la muerte de Bitcoin' (porque "nadie en su sano juicio va a querer gastar bitcoins").

14. Cada vez que el precio **baja considerablemente** se alzan voces que auguran 'la muerte de Bitcoin' (porque "nadie en su sano juicio va a querer conservar bitcoins").

15. Los **bloggers** más osados directamente dan por muerto a Bitcoin (algunos por tercera y hasta cuarta vez en menos de un año).

16. Algunos comerciantes de cierta envergadura se interesan en los beneficios de Bitcoin (ventajas competitivas; más clientes potenciales; eliminación de comisiones y reintegros involuntarios, etc.) y empiezan a aceptar bitcoins, aunque en su mayoría todavía fijan los precios en dólares o en la moneda local.

17. Proliferan los servicios que sólo aceptan bitcoins. En algunos nichos, las ventajas que ofrece Bitcoin resultan insuperables: prosperan especialmente los videojuegos online; los juegos de azar online; los sitios de compra y venta de bienes virtuales; los servicios online; los servicios de *hosting* anónimo; los proveedores de Internet que no almacenan datos de sus clientes, entre otros.

El futuro (según los autores de este libro)…

18. En medio de una recesión mundial que sigue profundizándose, un importante fondo de inversión identifica a Bitcoin como posible refugio de valor. El precio del bitcoin aumenta bruscamente.

19. Un político de renombre acusa a los usuarios de Bitcoin de terroristas, traficantes de armas y adictos a las drogas y a la pornografía infantil. Los noticieros televisivos (que a esta altura son prácticamente organismos del Estado) se hacen eco. Cunde el temor a alguna forma de intervención gubernamental. El precio del bitcoin cae bruscamente.

20. El núcleo duro de usuarios de Bitcoin es lo suficientemente numeroso como para mantener saludable a la nueva economía.

21. La crisis económica mundial tiene a los políticos demasiado preocupados como para tratar de entender qué cosa es Bitcoin. Con el fin de sobrevivir a la gran depresión, los estados se ven obligados a achicarse y pierden influencia. Ya nadie se acuerda de las leyes "antipiratería" – aunque teóricamente siguen vigentes – y a nadie se le ocurre intentar combatir el uso de Bitcoin por vía legal.

22. Surgen los primeros servicios de remesas especializados en transferir fondos internacionalmente por medio de Bitcoin.

23. Se difunde entre banqueros y funcionarios públicos de alto rango un informe confidencial que explica por qué Bitcoin

es imparable, indestructible e incontrolable. Los asesores financieros de la vieja élite recomiendan a sus clientes adquirir algunos bitcoins para protegerse de la depreciación de sus activos. El precio del bitcoin se triplica en el curso de una semana, despertando la curiosidad del mundo entero.

24. Millones de comerciantes añaden a Bitcoin como medio de pago. Ante las ventajas que brinda la nueva moneda digital, muchos deciden ofrecer importantes descuentos a quienes paguen con bitcoins.

25. La propuesta de usar a Bitcoin como sistema monetario en una ciudad libre (de interferencia estatal) empieza a ser considerada en círculos libertarios.

26. Tras una prolongada etapa de hiper-deflación, el dinero de curso forzoso empieza a circular nuevamente, y en cuestión de meses el mundo entero cae presa de un agudo proceso inflacionario. Extremadamente endeudados, los gobiernos apelan a la emisión monetaria para enfrentar las obligaciones contraídas, destruyendo así el poder adquisitivo de la población.

27. El dinero de curso forzoso pierde todo su valor, en medio de una hiperinflación que alcanza al mundo entero. El oro, la plata y Bitcoin se convierten en los únicos refugios de valor confiables. Los jubilados caen en la cuenta de que los gobiernos se han gastado todo el dinero que les habían prometido. Desesperados, muchos recurren al trueque para sobrevivir.

28. Pero una era de prosperidad está a punto de emerger de las ruinas de la civilización…

29. Puesto que no hay una autoridad central emitiendo ni creando bitcoins arbitrariamente, la banca de reserva fraccionaria se vuelve marginal – si no inviable –, y el valor del bitcoin aumenta de manera constante – a la par de la productividad mundial.

30. El oro y la plata se utilizan también como sustitutos del dinero en efectivo y como instrumentos para preservar el valor, pero la gran mayoría de las transacciones tienen lugar en bitcoins. El valor del bitcoin aumenta exponencialmente.

31. Un bitcoin alcanza para comprar una manzana entera de una ciudad, con todos sus bienes muebles e inmuebles. El microbitcoin (una millonésima parte de un bitcoin) es la unidad de valor generalmente utilizada para referirse a grandes transacciones comerciales.

32. La planificación central de las tasas de interés desaparece junto con los bancos centrales. Esto mejora drásticamente la asignación de recursos en el sector privado, y le permite a la economía desplegar todo su potencial.

33. Al no haber estados capaces de financiarse violentamente para despilfarrar la riqueza, la productividad global crece tanto que a la mayoría de las personas le alcanza con trabajar unas pocas horas a la semana. Todas las energías de la humanidad pasan a servir a los intereses del consumidor a través del libre intercambio.

34. Ya no hay guerras ni dictaduras militares, dado que éstas no pueden existir sin la facultad de robarle a la gente el fruto de su trabajo.

Buscando a Satoshi Nakamoto

Dos periodistas norteamericanos se han propuesto recientemente, cada uno por su lado, develar la identidad del creador de Bitcoin. La tarea no es para nada sencilla, y en el mejor de los casos todo quedará en meras hipótesis.

Según parece, Satoshi se ha ocupado de borrar cualquier rastro que pueda conducir a su verdadera identidad, y no tiene la menor intención de darse a conocer ante un periodista. De modo que a esta altura ya nadie espera una confesión espontánea de parte de (quien sea en realidad) Satoshi Nakamoto.

Estos dos periodistas eligieron estrategias diferentes para dar con el genio detrás del famoso pseudónimo: uno de ellos, tras una larga investigación, decidió centrarse en una cumbre de especialistas en criptografía; el otro partió de una serie de pistas encontradas en el ***paper*** inaugural de Bitcoin, firmado por Satoshi Nakamoto.

Hasta ahora, el abanico de sospechosos se reduce a unos pocos individuos, ninguno de los cuales admite siquiera haber colaborado en algún aspecto del proyecto Bitcoin. Pero los atributos y los conocimientos que reúne Satoshi Nakamoto son tan extraordinarios, y tan raramente hallados en una misma

persona, que algunos sugieren que Satoshi Nakamoto es en realidad un grupo de personas.

SEGUNDA PARTE

LA IMPORTANCIA DE BITCOIN

Satoshi Nakamoto, un Gutenberg del siglo XXI

Bitcoin es al dinero de curso forzoso lo que la imprenta de Gutenberg fue, en el siglo XV, al monopolio sobre el saber escrito. Así como la imprenta de tipos móviles llevó la palabra escrita – para horror de los poderosos de turno – a todos los rincones del mundo, Bitcoin tiene hoy el potencial de liberarnos de la servidumbre que facilita, en todos los rincones del mundo, la manipulación monetaria.*

Al permitirnos acceder a una tecnología que hasta ahora había sido utilizada en nuestra contra, y hacer uso de ella para defender nuestra soberanía individual, Bitcoin ha cambiado para siempre las reglas del juego.

Una vez más, el ingenio humano se alza frente al privilegio establecido por la violencia, y al hacerlo nos deja ver la naturaleza del sistema que se nos ha impuesto.

** El dinero de curso forzoso es la causa principal de – entre otros males – el hiperendeudamiento estatal, el ciclo económico, la inflación, la pobreza y la guerra.*

El valor de Bitcoin

No está de más repetirlo, ya que incluso algunos partidarios de la libertad monetaria parecen confundidos al respecto: **el valor de Bitcoin es una función de sus cualidades monetarias**.

Una moneda es mejor que otra **no** porque lo hayan dispuesto las autoridades, sino porque nos es más útil, porque es una **mejor herramienta** - así como un martillo de acero es mejor herramienta que un martillo de papel, aunque el segundo lleve impreso el rostro de un monarca.

Sin embargo, en cuestiones monetarias el sentido común está virtualmente prohibido. **Nos han enseñado que el valor de la moneda proviene de un mandato gubernamental**; que "nuestro" signo monetario debe ser un motivo de

orgullo; que sin dinero estatal no hay mercado posible; que la inflación es el motor de la economía; que un prócer nos vigila desde cada billete por si olvidamos que **el fruto de nuestro trabajo no nos pertenece**.

¿Hace falta señalar que nos han mentido? Y son esas mentiras - creídas por una clase productiva pero económicamente iletrada - las que aún le dan sustento a la mayor estafa de la historia. Según el relato oficial, la institución moneda nació con el Estado: en ausencia de respaldo legal, por caso, el valor de una onza de oro no sería más que una ilusión colectiva. ¿Y el valor de un bitcoin? Una broma de mal gusto - ni siquiera una ilusión.

Dejemos que lo crean, mientras la adopción de Bitcoin se expande en todas direcciones. Cuando finalmente comprendan por qué tanta gente prefiere a Bitcoin, será muy tarde para frenar el avance de la cadena de bloques.

El triunfo de la no-violencia

El espectáculo de algo que funciona puede ser hipnótico. Con frecuencia los resultados – inmediatos, concretos, maravillosos – opacan el contexto que los hace posibles. ¿Bajo qué condiciones funciona lo que funciona?: si somos incapaces de identificarlas, somos incapaces de aprender, lisa y llanamente. Ignorar las relaciones causales, los principios subyacentes, nos condena a las tinieblas, al temor a fuerzas enigmáticas, a la exigencia y a la súplica impotente… a bailar la danza de la lluvia en un mundo incomprensible.

En el fondo lo sabemos, todos lo sabemos: a escala social, un sistema funciona – disemina la prosperidad, aumenta la productividad – en la medida en que somos libres de hacerlo funcionar: libres de crear, de innovar, de ofrecer, de persuadir, de intercambiar… en fin, de interactuar para el mutuo beneficio. El requisito es la libertad. Es así de simple. La mente humana no puede ser forzada a trabajar como una bestia de carga.

Lo que funciona, entonces, funciona **a pesar** de la violencia. Los seres humanos pueden producir – a regañadientes – bajo amenaza, pero jamás motivados por la amenaza. Nuestros amos lo saben, por eso intervienen toda vez que algo parece funcionar. El propósito de la intervención estatal es, precisamente, que eso deje de funcionar, para demostrarnos que ningún proyecto es viable al margen del Estado. Afirmar lo contrario equivale a

cuestionar la razón de ser del Estado; y actuar en consecuencia… está prohibido.

El largo brazo de la ley, con su puño de acero, provee la ilusión de control y eficacia en el corto plazo, pero siempre falla en el largo plazo. Tiempo atrás, advertir el fracaso de la violencia estatal solía requerir generaciones. Hoy, la aceleración que impone Internet evidencia el fracaso de la violencia en plazos cada vez más cortos. Nunca antes la interacción entre seres humanos había sido tan veloz, tan espontánea e incontrolable, y por ende tan eficaz. Como siempre, menos violencia es igual a mejor funcionamiento.

Más violencia, en cambio… La violencia es tan eficaz para resolver un problema social como lo es la danza de la lluvia para resolver un problema de sequía. ¿Caerá en desuso, también? Al fin y al cabo, el estatismo es tan sólo el fruto más popular del pensamiento mágico-religioso. Creer que una economía entera puede funcionar a punta de pistola es, para el estatista, la prueba de fe por excelencia.

El estatista pide siempre más violencia; a él no se le ocurre otra solución para los problemas – económicos o de cualquier otra índole –; no se le ocurre que la violencia está en la raíz de esos mismos problemas. En efecto, lo único que debiera sorprendernos de los recurrentes colapsos financieros es que aún sorprendan a alguien. Porque nadie ignora que el aspecto más socializado de nuestra economía – el más sometido a coacción – es justamente el más importante: el sistema monetario.

Pero nos hemos acostumbrado a ser tratados como ganado. Tanto tiempo nos han restringido, y reprimido, y tan duro nos han castigado por hacer lo correcto… que el espectáculo de un libre mercado sin fricciones nos produce vértigo. Como aquellos soviéticos que tras la caída del muro se preguntaban: ¿y ahora quién repartirá el pan?, nosotros nos preguntamos: ¿es posible un libre mercado monetario? Bueno, su manifestación más conspicua ya está entre nosotros, y es refractaria a la violencia estatal.

En el mundo Bitcoin no hay – ni puede haber – élite gobernante, ni cadena de mandos, ni afiliación compulsiva, ni licencias obligatorias, ni aduanas, ni regulaciones arbitrarias… de modo que las soluciones a los diferentes problemas no demoran en gestarse y propagarse, y no encuentran barreras artificiales.

El muro ha caído. La libertad funciona.

Hacia la separación entre Moneda y Estado

Cuando se habla de los puntos débiles de Bitcoin, en realidad ya casi no se habla de Bitcoin, sino de sus puntos débiles **en relación al Estado**: "¿hacia dónde apuntaría una eventual prohibición de Bitcoin?"; "¿qué idearán los servicios de inteligencia para entorpecerlo?"; "¿qué estrategias adoptarán para limitar su expansión?", etc.

Pero el Estado – una tecnología que se viene empleando desde hace unos cinco mil años – parece haber encontrado en Internet un obstáculo infranqueable. Gracias a Internet, juventud e inteligencia ya no equivale a desventaja y aislamiento… ¡sino todo lo contrario! Gracias a Internet, explosión de productividad no significa necesariamente explosión del poder estatal… ¡por primera vez en la historia de la humanidad!

En el futuro, los historiadores situarán a Bitcoin en los albores de un proceso inevitable: la separación entre Moneda y Estado. Hay una gran diferencia entre este fenómeno y su destacado precedente, la separación entre Iglesia y Estado: el Estado puede subsistir sin casta religiosa… pero no sin moneda de curso forzoso.

Cómo nos beneficia Bitcoin

El mejor sistema de organización social **no es** aquél teóricamente capaz de predecirlo todo y de establecer qué tenemos que hacer, cómo tenemos que hacerlo y cuándo tenemos que hacerlo. No importa cuánta tecnología le arrojemos a un sistema social basado en una mala teoría; sus resultados serán siempre catastróficos. Por supuesto, eso no le impide a una nueva generación de tecno-utopistas presagiar un futuro gobierno de máquinas providenciales que – esta vez sí – abolirán todos nuestros problemas. Si esto suena extrañamente familiar, es porque se trata de una versión más – esperemos que la última – del colectivismo, y como tal no hace más que volver a expresar la nostalgia de un pasado tribal – de un jefe sabio y todopoderoso; de una tradición que dé cuenta de todo.

El mejor sistema de organización social es aquél que funciona merced a unas reglas sencillas, estables y aceptadas de buen grado por todos los participantes; aquél que provee un marco dentro del cual cada uno es libre de hacer lo que quiera, excepto eludir las consecuencias de sus actos. La prosperidad y la justicia son simples corolarios de tal sistema.

Un sistema monetario como Bitcoin, cuyas reglas premian la conducta mutuamente beneficiosa y desincentivan fuertemente la usurpación y el fraude, hace prácticamente imposible la falsificación, la inflación y el endeudamiento en nombre de otros (y por ende prohíbe los proyectos faraónicos y las guerras, entre otros pasatiempos gubernamentales).

Pero Bitcoin no tiene que ser un sistema perfecto; tan sólo tiene que ser mejor que las alternativas monetarias hoy disponibles para llegar a ser ampliamente aceptado. En rigor, ningún aspecto de Bitcoin puede ser considerado perfecto, pues está en su naturaleza evolucionar constantemente.

Desde un punto de vista económico y técnico, Bitcoin ya es infinitamente superior al sistema monetario vigente. También lo es desde un punto de vista moral, y esto explica por qué, a pesar de todas sus ventajas, hay quienes se oponen a Bitcoin.

Los perjudicados

Los perjudicados por una futura expansión viral de Bitcoin serían, en realidad, quienes ya no estarían en condiciones de perjudicar tan fácilmente a los demás para su propio beneficio:

- Políticos que buscan endeudarse a expensas de la población productiva (presente y futura).
- Funcionarios públicos dedicados a manipular el sistema monetario y a imponer el dinero (devaluado) de curso forzoso.
- Banqueros (bajo el actual marco regulatorio).
- Empresarios prebendarios.
- Empleados y toda clase de personal cuyos beneficios dependen exclusivamente del Estado o bien de regulaciones gubernamentales.

- Economistas que defienden el sistema vigente para mantener sus puestos académicos o administrativos.
- Dependencias estatales y compañías que se dedican a recolectar información de los consumidores.
- Quienes han invertido excesivamente en dinero de curso forzoso.
- Gente acostumbrada a gastar por encima de sus ingresos.
- Ladrones.
- Falsificadores.
- Servicios caros, ineficientes y centralizados de pago y transfeencia de dinero (*Western Union*, tarjetas de crédito, *PayPal*, etc.).

Los adictos a la violencia institucionalizada tienen mucho que perder con el éxito de Bitcoin (y de cualquier otro sistema que demuestre la infinita superioridad de la organización voluntaria). Por lo tanto, no esperemos que los medios masivos de comunicación nos cuenten sin rodeos las ventajas de Bitcoin, ni esperemos que la expansión de Bitcoin se produzca sin una fuerte resistencia.

Si algo ha demostrado la Historia es que nadie renuncia ligeramente a sus privilegios.

El lugar de Bitcoin en la Historia

Algunos autores sitúan a la irrupción de Internet en los albores de una nueva era, como un paso evolutivo comparable a la adquisición del lenguaje. En efecto, tanto el lenguaje como Internet son **sistemas abiertos, descentralizados, organizados de manera espontánea, y refractarios al uso de la fuerza**. Y es precisamente la naturaleza ingobernable de ambos la razón de su dinamismo, de su resistencia y de su enorme poder transformador.

Basta comparar la situación de los primeros hombres en dominar el lenguaje

con la de sus coetáneos, obligados a transmitir emociones e ideas muy simples por medio de gestos y sonidos guturales – más que de un paso hay que hablar de un **salto evolutivo** entre la comunicación rudimentaria y el nivel de abstracción que habilitó, por primera vez, el libre intercambio de ideas y productos. Recién entonces la inteligencia logró alzarse ante la brutalidad, oponiendo el comercio con el extranjero a la hostilidad y el saqueo; oponiendo, en definitiva, las relaciones voluntarias al uso de la fuerza.

También **Internet ha llevado la comunicación a otro nivel**. Empero, así como la ausencia de una lengua franca limita seriamente las posibilidades del lenguaje humano, la ausencia de una moneda digital descentralizada y de uso voluntario mantiene a Internet bajo el asedio de barreras políticas – todas completamente absurdas y corruptas – que introducen fricción en los intercambios, cuando no los impiden.

No es exagerado decir que Internet estaba esperando a Bitcoin para empezar a desplegar todo su potencial.

Un sistema monetario a la altura de Internet

Exigir que millones de personas renuncien a intercambiar información por medio de Internet (o bien que soliciten autorización antes de hacerlo) equivale a exigir que vuelvan a caminar en cuatro patas.

¿Por qué habrían de renunciar a las infinitas posibilidades que estas ventajas evolutivas han originado? La mayoría se resistirá. Y quienes obedezcan, lo harán no sólo en contra de sus propios intereses; estarán enfrentándose a una tendencia tan elemental que es compartida por todos los organismos vivos.

Una vez adquirida cierta ventaja evolutiva – sea esta la marcha bípeda, el lenguaje simbólico o el acceso a toneladas de información en una fracción de segundo – ya no hay vuelta atrás. Cuando una ventaja es tan categórica, lo normal es que se propague hasta convertirse en el nuevo estatus del que todos pueden gozar.

Habiendo soportes digitales y medios que permiten compartir instantáneamente imágenes, textos, sonidos y videos con casi todos los habitantes del planeta, no alcanzará la fuerza de mil ejércitos para obligarnos a volver a utilizar cassettes, o a comprar los treinta y dos tomos de la

Enciclopedia Británica.

Tal como le ha tocado en su momento a los fabricantes de velas – ante la expansión de la luz eléctrica –, toda la industria de la música se ha tenido que adaptar a un mundo cambiante. Lo mismo tendrán que hacer de aquí a poco los grandes decisores de Hollywood, sólo para no condenarse a la intrascendencia. El mundo simplemente no se adaptará a ellos. Y no importa cuánto dinero ni cuántas conexiones políticas tengan; si no admiten la derrota de su modelo de negocio, las nuevas generaciones ni siquiera sabrán de su existencia, y hasta los analfabetos tecnológicos se reirán de sus amenazas.

Los bancos también tendrán que adaptarse o caer – su alianza con los estados no está escrita en el firmamento. Al fin y al cabo, lo que se transmite por medio de Bitcoin es información digital, y someter a los bits a un control arbitrario, en la era de Internet, no ha funcionado – ni funcionará – para los gobiernos, ni para las compañías discográficas, ni para los medios masivos de comunicación, ni para las agencias de viajes, ni para los servicios postales…

La tecnología es tan natural para el ser humano como lo es la marcha bípeda o el lenguaje simbólico. Por eso, impedir la innovación tecnológica siempre ha resultado, a la larga, una empresa inútil. Hoy, gracias a Internet, es también una empresa inviable.

La batalla por una Internet libre no se dará en los tribunales

La represión de la libertad de acceso a la información le dio impulso a *BitTorrent*, a *Wikileaks* y a millones de blogs que no responden a intereses gubernamentales ni corporativos. La represión de la libertad monetaria nos trajo a Bitcoin. Este es un proceso inexorable, que seguirá dándose una y otra vez frente a cada intento de controlar Internet.

Evidentemente, la batalla por la libertad no se librará en los tribunales. Ni siquiera debería librarse una batalla contra los poderosos de turno, pues no tiene sentido luchar por el reconocimiento de nuestras libertades. ¡¿Cómo?!

La corrupción y el creciente intervencionismo estatal no son perversiones del Estado; son, respectivamente, su esencia y su propósito. Por lo tanto, combatir los abusos del Estado con los medios del Estado es tan práctico y razonable como usar una guillotina para aliviar el dolor de cabeza. El propósito de la guillotina es matar, se diga lo que se diga en su defensa.

Así como lo contrario de la violación es la relación sexual mutuamente consentida, y no la violación con penetración limitada, lo contrario de la coacción estatal no es menos coacción estatal, sino relaciones libres y voluntarias entre seres humanos. *

¿Utópico?… cotidiano mejor dicho, además de legítimo, eficiente, viable y a nuestro alcance.

Si no queremos que los gobiernos atenten contra nuestras libertades, dejemos de implorarles que las reconozcan y que las protejan… y seamos libres.

Los políticos no van a renunciar a la violencia si nosotros no renunciamos antes a la esperanza en la política.

* *Versión en español de un ejemplo ideado por el filósofo canadiense Stefan Molyneux.*

TERCERA PARTE

ECONOMÍA

I - Bitcoin como moneda

Medio de intercambio y preservación del valor

Algunos escépticos dicen que no van a tomar a Bitcoin en serio hasta que una masa crítica de empresarios decida finalmente aceptar esta nueva moneda a cambio de sus productos. Ellos ven una economía creciente pero todavía inmadura en torno a Bitcoin (sin ver que, por eso mismo, abundan en ella las oportunidades), incapaz de respaldar la adopción de un nuevo medio de intercambio indirecto.

Pero lo cierto es que el éxito de Bitcoin no depende exclusivamente de sus virtudes como medio de intercambio indirecto: la preservación del valor (otra función monetaria) puede llegar a ser aún más importante.

De hecho, hoy en día son muy pocos los comerciantes que aceptan oro como medio de pago, no obstante lo cual nadie se atreve a cuestionar el lugar que ocupa el oro entre las monedas por excelencia.

Un sistema de incentivos no contrapuestos

Bitcoin, como señalan hasta sus enemigos, premia el ahorro. El ahorro, como saben hasta los que juntan monedas en un chanchito, es condición indispensable para la inversión. La inversión, como admiten hasta los marxistas, permite adquirir y aprovechar el capital, y como entienden hasta los keynesianos, impulsa la productividad – que es, a su vez, la explicación misma de la prosperidad.

No hay magia, sino conducta humana perfectamente racional, en cada uno de dichos eslabones. Si un sistema mantiene alineados los incentivos individuales, todos cumplirán de muy buen grado con las reglas establecidas, ya que el costo de violarlas excedería ampliamente a los beneficios potenciales.

En cambio, en un sistema que determina incentivos económicos contrapuestos (como el sistema monetario vigente: coactivo, centralizado, vertical, inflacionario), la conducta humana perfectamente racional no derivará

en prosperidad sino en pobreza para el conjunto: “¿para qué ahorrar si mis ahorros pierden valor?”; “¿para qué esforzarme si puedo vivir del esfuerzo ajeno?”; etc.

Imponerle a un tercero los costos de un conflicto, un negocio o un contrato, con el fin de satisfacer a las partes involucradas, es algo tan inmoral como socialmente destructivo. Sin embargo, eso es todo lo que podemos esperar del Estado.

Pero el inicio del uso de la fuerza no es – ni ha sido jamás – necesario ni justificable. Y ahora, para la economía que florece bajo las reglas de Bitcoin, tampoco es ni será posible.

¿“Tan sólo” la primera moneda digital descentralizada?

- Por algún motivo, muchos analistas del fenómeno Bitcoin comparten la opinión de que éste es un interesante experimento monetario, pero que tan sólo es el primero en su género. Ellos vislumbran una larga serie de tentativas, cada vez más acertadas, de reemplazar al dinero de curso forzoso. Sin embargo, para sostener dicha conjetura es necesario ignorar lo siguiente:

- La competencia entre monedas libres (no impuestas por la fuerza) tiene características particulares: el grado de aceptación voluntaria de una moneda es un factor que no puede ser subestimado a la hora de explicar su adopción. La mejor moneda es masivamente adoptada por ser la mejor moneda, y también es la mejor moneda porque ha sido masivamente adoptada. Debido a las consecuencias de este bucle de retroalimentación positiva es que difícilmente lleguen a existir “miles de sistemas monetarios” compitiendo por destronarse mutuamente.

- Cuanto más tiempo pasa demostrando su solidez, más confiable se torna el sistema monetario predominante – y menos probable su reemplazo por otro sistema que aún no ha superado la prueba del tiempo.

- La multiplicidad de signos monetarios nacionales es un efecto de la intervención estatal, no del libre juego de la oferta y la demanda. Cuanta más gente pueda elegir en qué moneda negociar, calcular y ahorrar, más se extenderá la adopción de la mejor moneda disponible. Quizás Bitcoin se

convierta, con el tiempo, en la base universal de otros sistemas de dinero digital (limitados a grupos humanos con altos niveles de confianza mutua).

- Para superar a Bitcoin no basta con introducir alguna que otra “mejora” en su protocolo y lanzarlo con otro nombre: el *software* puede ser copiado y modificado, pero el ecosistema que sigue desarrollándose en torno a Bitcoin (programadores, comerciantes, consumidores, emprendedores, mineros, operadores, ahorristas, etc.) es mucho más difícil de reproducir.

- Bitcoin siempre estuvo, está y estará abierto a la innovación: para mejorar algún aspecto del sistema no es necesario reemplazarlo por un sistema alternativo. Si se tienen buenas ideas y capacidad para la manipulación programática, es más económico y productivo unirse al proyecto Bitcoin que dedicarse a crear otra moneda digital descentralizada.

Bitcoin versus oro

I

Las grandes creaciones monetarias no son precisamente frecuentes. Miles de años atrás, el primer individuo en descubrir y aprovechar las cualidades monetarias del oro no imaginó la magnitud de la explosión productiva que había desencadenado. De hecho, gracias a sus propiedades fisicoquímicas, a su amplia distribución geográfica y a su baja proporción entre producción anual y stock de existencias, el oro sigue siendo la moneda por excelencia – y acaso el único medio confiable para extinguir deuda en un contexto como el actual.

El oro superó con creces la prueba del tiempo debido a que cumple muy bien con sus funciones monetarias – lo cual no significa que es insuperable. Veamos algunos de los inconvenientes que presenta el oro como medio de intercambio y preservación del valor:

- Es relativamente fácil de falsificar.
- La cantidad de oro en una moneda puede ser alterada.
- Las pequeñas unidades (Ej.: milésima parte de una onza) no son

convenientes para el intercambio cotidiano.

- Con el uso frecuente pierde algo de valor debido a la abrasión.
- Es difícil transportar grandes cantidades de forma segura.

Bitcoin es objetivamente mejor moneda que el oro, así como el oro es objetivamente mejor moneda que la sal. ¿Por qué, entonces, Bitcoin no es tan ampliamente aceptado como el oro? Por la misma razón que, en el año 1974*, el correo electrónico no era tan ampliamente aceptado como el correo postal.

**El correo electrónico fue creado en el año 1971.*

II

Tras más de cinco mil años de uso, el oro sigue vigente. Más allá de los avances en materia de acuñación (escasos) y extracción (poco relevantes desde el punto de vista monetario), la tecnología no ha cambiado las propiedades que hacen "precioso" a este metal.

El éxito del oro se debe en gran medida a un atributo que comparte con Bitcoin: su naturaleza descentralizada. Nadie puede monopolizar su producción, ni controlar su "emisión". Sin embargo, mientras que las unidades de oro no pueden ser replicadas, los recibos de pago en oro sí pueden serlo. Así, toda vez que – por su practicidad – se hace necesaria la circulación de letras de cambio nominadas en oro, el antiguo problema del doble gasto reaparece.

El problema del doble gasto se resuelve parcialmente acudiendo a organizaciones que garanticen la legitimidad de cada transacción. De esta forma, la circulación de recibos con respaldo en oro pasa a ser el lubricante de los mecanismos que hacen funcionar a una economía compleja. ¿Obstáculo superado? Lamentablemente no: cualquier sistema monetario basado en cámaras de compensación o puntos de intercambio más o menos centralizados está expuesto a la hostilidad gubernamental y es vulnerable a toda clase de fraudes.

En el caso de Bitcoin, unidad y recibo son una misma "cosa" imposible de replicar o falsificar. Esta mutación radical de lo que entendemos por moneda

permite que las transacciones se lleven a cabo sin la necesidad de confiar en terceros, y sin obstaculizar el comercio.

III

Para que un bien sea económicamente valioso, tiene que ser a la vez útil y escaso (al menos en un determinado contexto). La utilidad no alcanza: el aire no sólo es útil, es absolutamente indispensable; sin embargo, al ser abundante y ubicuo – exceptuando circunstancias extraordinarias – no le asignamos un valor económico. La escasez tampoco es suficiente para condicionar el valor económico de un bien: los pelos de la barba del panadero de la esquina son escasos, pero no por eso tienen un valor económico.

Lo dicho explica por qué el precio del oro tiende a ser más elevado que el precio del agua, siendo el agua un bien indispensable. **La utilidad de los bienes decrece a medida que aumenta su cantidad disponible, de modo que valoramos menos cada unidad adicional de un determinado bien**. Veamos un ejemplo: si tenemos sed, el primer vaso de agua lo usaremos para hidratarnos; el segundo vaso puede que lo usemos para regar las plantas; el tercero quizás lo destinemos a la cubetera de hielo, y el cuarto posiblemente a mantener cargada la pistola de agua. A este fenómeno se refiere el concepto de utilidad marginal decreciente.

Dadas sus cualidades, **el oro es considerado el bien cuya utilidad marginal disminuye más lentamente**. En otras palabras: cada unidad adicional de oro tendrá casi tanta utilidad para quien la posea – y será valorada casi tanto – como la unidad anterior. Esto diferencia al oro de otros bienes menos líquidos, es decir menos aptos para funcionar como medios de intercambio.

Ahora bien, si la lentitud con que disminuye la utilidad marginal de un bien es lo que define su condición de buena moneda… ¿qué hay de Bitcoin? Es cierto que el oro prácticamente no se deteriora con el paso del tiempo, pero también es cierto que tener más unidades de oro implica un costo más elevado de almacenamiento (o bien asumir el riesgo de perder una mayor cantidad de oro). En este sentido, **cabe decir que la utilidad marginal de Bitcoin es constante, y, por lo tanto, que Bitcoin es mejor moneda que el oro**.

La tibieza de los intelectuales

Un espectáculo curioso dan quienes debaten teorías a ojos cerrados: que Bitcoin no es técnicamente moneda; que no tiene "valor intrínseco"; que no encaja en el teorema de la regresión de Mises…

¡Pobre Mises!; debe estar revolcándose en su tumba… Si lo hubieran leído, sabrían que el famoso teorema no se aplica a la moneda en general, sino a los metales preciosos, y que para él **la evidencia empírica tiene el poder de arrasar con la más elegante de las teorías**.

¿Para qué argumentar en contra de una teoría según la cual Bitcoin no puede funcionar, cuando hay una economía floreciente basada en Bitcoin? **Dejemos que la realidad sea nuestro argumento**; dejemos que los intelectuales libertarios se entretengan discutiendo lo que hubiera pensado Mises, Hayek o Rothbard acerca de Bitcoin, mientras todo un ecosistema informático y una nueva economía global se despliegan ante sus narices.

Ningún otro sistema tiene el potencial de Bitcoin para materializar aquella libertad monetaria que tanto pregonan los intelectuales libertarios. Ante semejante oportunidad, que ellos no estén celebrando unánimemente es algo curioso; pero que se aferren a teorías falsas (¡valor intrínseco!) con tal de impugnar a Bitcoin… es sintomático.

¿Acaso los intelectuales libertarios aprecian más la seguridad de sus puestos académicos (garantizada por el Estado) que las libertades que dicen defender? Eso explicaría sus absurdos remilgos teóricos.

Los diferentes roles en la nueva economía

Casi todos los usuarios de Bitcoin han asumido – de manera simultánea o sucesiva – más de un rol en esta nueva economía. Veamos a qué se dedican los integrantes de la comunidad Bitcoin:

Pioneros en la adopción de Bitcoin:

Los ***early adopters*** de Bitcoin se sumaron al proyecto cuando éste no era

más que un sueño, dándole el impulso inicial para que sobreviva a las primeras etapas de su desarrollo. Ellos apostaron a Bitcoin en contra de todos los pronósticos – y ganaron. Hoy, muchos ***early adopters*** encabezan o financian emprendimientos relacionados con Bitcoin.

Mineros:

Al verificar la legitimidad de las transacciones, los mineros proveen seguridad a todos los usuarios de Bitcoin. Para eso invierten su tiempo (en actualizar, mantener y ajustar sus equipos) y su dinero (en hardware y electricidad). Lo hacen, por supuesto, a cambio de una recompensa en bitcoins.

Desarrolladores:

El ecosistema informático que se ha gestado en torno a Bitcoin requiere de programadores altamente motivados en todos sus niveles. La velocidad a la que ellos resuelven los problemas y amplían nuestras posibilidades es tan asombrosa que las alternativas a Bitcoin parecen alejarse cada vez más en la prehistoria de los sistemas monetarios.

Especuladores:

Actividad incomprendida si las hay, la especulación monetaria es la razón por la cual el precio del bitcoin se ha mantenido en un rango cada vez más estrecho. Cuantos más especuladores haya (en un mercado libre), más costosa resultará la manipulación monetaria, y, por ende, más estable será el precio. Además, al ofrecer su capital en los mercados cambiarios, los especuladores proveen liquidez a los usuarios de Bitcoin en todo el mundo.

Ahorristas:

Creen en Bitcoin, y lo demuestran atesorando buena parte de los bitcoins que han adquirido. De esta manera, mejoran el poder adquisitivo de todos los poseedores de bitcoins (muchos de los cuales invertirán ese capital en emprendimientos que, a larga, fortalecerán a Bitcoin), y así atraen a nuevos usuarios. Al arriesgar su propia riqueza a cambio de una recompensa futura que no está garantizada, los ahorristas traen al presente una parte de ese valor futuro que han pronosticado.

Comerciantes:

Desde los emprendedores más arriesgados hasta los comerciantes más tradicionales, todos los que aceptan bitcoins a cambio de sus productos están expandiendo el uso y difundiendo las ventajas de la nueva moneda digital.

Consumidores:

Son quienes guían, en gran medida, las decisiones de los empresarios. Usar bitcoins para adquirir bienes y servicios es otra manera de fortalecer a la economía basada en Bitcoin.

El genio de Satoshi Nakamoto

El genio de Satoshi Nakamoto no reside únicamente en su originalidad, sino en haberse fijado en cómo funciona el mercado, y qué roles cumple en él la moneda, antes de crear un medio más eficaz y eficiente para cumplir con esas mismas funciones.

Satoshi no reinventó la moneda; lo que hizo fue entenderla, y luego mejorarla. La moneda es un instrumento con funciones muy específicas: facilitar el intercambio indirecto y la preservación del valor, además de servir como unidad de cuenta. Pedirle a la moneda que sea cualquier otra cosa es como pedirle a las manos que sirvan para caminar. Y ya lo dijo G. K. Chesterton: "Si camináramos sistemáticamente con las manos, éstas serían pies."

Como la creación de monedas digitales está hoy en día al alcance de cualquier programador, hay quienes piensan que pueden reformar la institución moneda para que cumpla con otros objetivos – los suyos, presuntamente muy nobles.

Algunos "innovadores" en el campo de la moneda nos piden que confiemos ciegamente en ellos (tal como hacen los gobiernos, aunque sin las armas para someternos a sus reglas). Otros nos proponen que dejemos constancia, en una serie de formularios, de qué es lo que más valoramos, y en quién confiamos, y cuánto nos agrada tal o cual persona – y por qué motivos –, etc., etc. Según estos últimos, no basta con haber aprendido a sumar y a restar para tener participación legítima en la institución moneda, sino que es necesario contar con una buena reputación en ciertas redes sociales. Por supuesto, jamás han

estudiado qué es la moneda, pero eso no les impide lanzarse a reformarla. Que quede claro: no es que no saben exactamente cómo funciona la moneda… ¡no saben lo que es!

Si un mecánico dice que es capaz de arreglar tu coche, aunque admite que no sabe cómo funciona, y afirma desconocer por completo el concepto de motor… ¿lo dejarías poner manos a la obra? Pues éste “mecánico” sería tan confiable como aquellos programadores que se lanzan a inventar (o a criticar) monedas digitales a pesar de que ignoran las nociones más elementales de la ciencia económica.

A diferencia de las monedas cuyos atributos debemos al azar (como el oro), de las monedas digitales centralizadas (como los *facebook credits*) y del dinero de curso forzoso (como el dólar), Bitcoin es el fruto de un diseño a la vez consciente, disruptivo y apoyado en teorías válidas. ¿Acaso no es esa la fórmula de toda gran creación?

Los forks: una advertencia

Un ***fork*** es un proyecto de software que parte de una copia de otro proyecto para desarrollarse independientemente del original. A la hora de justificar sus actos, los creadores de un *fork* suelen aducir motivos filosóficos o prácticos, pero no nos extenderemos en ellos. El propósito de este escrito es advertir al lector que los *forks* también pueden estar animados por malas intenciones y/o malas ideas. Ese ha sido el caso de los *forks* de Bitcoin hasta la fecha – y *Litecoin*, el último de la serie, no parece ser la excepción.

Forks en general

• Salvo que se esté trabajando en innovaciones revolucionarias, los esfuerzos dirigidos a crear un *fork* serían mejor invertidos en el desarrollo de Bitcoin. Hasta la fecha, los *forks* han dispersado unas energías de las cuales el proyecto Bitcoin podría beneficiarse, y han desaparecido (o están en trance de desaparecer) sin dejar ningún aporte valioso. Cabe sospechar que se trata en realidad de meras estafas, especialmente diseñadas para atraer a mineros e inversores que aspiran a convertirse en pioneros.

• Bitcoin siempre estuvo, está y estará abierto a la innovación, de modo que

para mejorar algún aspecto del sistema no es necesario reemplazarlo por un sistema alternativo.

• Ni siquiera una cantidad de ventajas técnicas respecto a Bitcoin serían suficientes para superar el peso de su amplia aceptación – y de todo lo que a su alrededor se ha desplegado (el vasto y complejo ecosistema de programadores, comerciantes, consumidores, emprendedores, mineros, operadores, ahorristas, etc.). La gente siempre tenderá a preferir, entre dos monedas, a la más líquida, vale decir a la que más fácilmente puede ser intercambiada, en todo momento, por cualquier activo.

• Bitcoin no tiene la supervivencia asegurada, pero si algún día llegara a viralizarse, los *forks* quedarían en un segundo o tercer plano indefinidamente (tanto la ***first mover advantage*** como el ***network effect*** jugarían a favor de Bitcoin), y si Bitcoin llegara a fracasar, los *forks* no tendrían la menor chance de sobrevivir a la extinción de Bitcoin.

• Bitcoin será el *gold standard* del futuro, o bien será reemplazado por algo muy (pero muy) superior.

Litecoin en particular

• Según sus creadores, Litecoin no pretende ser la competencia de Bitcoin, sino una suerte de complemento (como lo es la plata o el bronce en el contexto de un patrón oro). Pero dada la naturaleza de las criptomonedas, no tiene mucho sentido contar con un equivalente digital de la plata o el bronce. La divisibilidad del oro para el uso cotidiano tiene un límite; de ahí la utilidad monetaria de otros metales menos valiosos. Bitcoin, en cambio, es (en la práctica) infinitamente divisible.

• Usar simultáneamente bitcoins y litecoins implicaría una nueva serie de dificultades para la mayoría de los que recién están empezando a entender el funcionamiento de Bitcoin – y a gestionar sus billeteras.

• La minería de litecoins sólo es posible con CPU. Aunque esto se presenta como un punto a favor de Litecoin, en realidad es todo lo contrario. La apertura a la competencia tecnológica es un punto a favor de Bitcoin, pues la minería tiene un rol demasiado importante como para quedar arbitrariamente atada a un determinado estadío tecnológico. Por otra parte, si Litecoin llegara a popularizarse, el incentivo para superar los obstáculos impuestos a las formas

eficientes de minar pasaría a ser descomunal – y a jugar en contra de la viabilidad misma del sistema. Bitcoin, en cambio, premia la eficiencia y la especialización (dos factores clave para el progreso en todos los órdenes).

• La distribución inicial de litecoins es, de acuerdo a sus defensores, más equitativa, porque la minería con CPU también es viable en países pobres. Pero el éxito de una economía no se mide exclusivamente por su capacidad para producir commodities (ej. Venezuela, Argentina o los países árabes bañados en petróleo), sino fundamentalmente por su productividad (ej.: Japón, Israel, Singapur). Si Bitcoin llega a transformarse en el nuevo *gold standard*, los magnates no serán los mineros, sino quienes más valor económico aporten con su trabajo, estén donde estén.

• Las confirmaciones de Litecoin son más rápidas que las de Bitcoin, pero no tan seguras como las de Bitcoin (reconocido por los creadores de Litecoin). Por eso mismo, bastaría que los litecoins adquieran suficiente valor para que la gente empiece a demandar más confirmaciones (al menos cuando se trate de transacciones entre desconocidos), anulando la ventaja de un intervalo más breve entre confirmaciones. Además, ya contamos con al menos dos soluciones para el problema de la excesiva espera, y ambas son potencialmente adoptables por el común de los *bitcoiners*: las *green adresses* y las *e-wallets* seguras.

Por último, un mensaje dirigido a los que recién han descubierto a Bitcoin y creen haber perdido la oportunidad de ser "*early adopters*" : **el proyecto Bitcoin, con todo su gigantesco potencial, aún se encuentra en su primera infancia. Sepan que hoy todos somos pioneros en este campo.**

Ripple: ¿competencia o complemento de Bitcoin?

Lo interesante de Ripple es que, a diferencia de algunas monedas alternativas – como freicoin – no se basa en teorías refutadas hace 100 años, ni - como es el caso de litecoin - en copias descaradas de Bitcoin.

Ripple es un sistema de emisión y gestión del crédito basado en una red P2P. Cada uno de sus integrantes funciona como un banco autónomo con la capacidad de extender y recibir crédito (nominado en diferentes monedas), y de hacerlo circular.

J P Koning acierta al comparar a Ripple con el sistema de letras de cambio que prosperó especialmente en los siglos XVII y XVIII. Estos papeles eran emitidos como un compromiso de pago a cambio de algún producto, y luego eran endosados por una larga cadena de comerciantes antes de alcanzar su madurez. Finalmente, el emisor cumplía con su promesa de pagar en oro el valor nominal de la letra de cambio.

Habida cuenta de su destacado precedente, Ripple tiene sin duda un gran potencial como instrumento facilitador de los intercambios. Pero afirmar que Ripple va a competir con Bitcoin es tan descabellado como afirmar que el email acabará compitiendo con Bitcoin.

Ocurre que Moneda y Crédito son instituciones fundamentalmente diferentes: la primera funciona en base a reglas abstractas; la segunda involucra relaciones y acuerdos personales.

Veamos qué propiedades de Bitcoin le faltan a Ripple:

- El usuario de Bitcoin no corre ningún riesgo de contraparte, lo cual significa que el valor de sus bitcoins no depende de la capacidad de algún tercero para cumplir con los compromisos que ha contraído. En este sentido, Bitcoin es comparable al oro, un medio de intercambio que no por nada sigue vigente luego de 5000 años de uso ininterrumpido.

- Los bitcoins son fungibles, vale decir que cada bitcoin tiene un valor igual al de cualquier otro bitcoin. La fungibilidad es una propiedad básica de la buena moneda que el crédito – dada su naturaleza – no tiene ni puede tener. Para que circule de manera eficiente, el crédito debe ser medido en unidades fungibles.

- Bitcoin está diseñado para funcionar como medio de intercambio y preservación del valor. Como la historia del dinero estatal ha demostrado una y otra vez, los medios de intercambio que no facilitan, asimismo, la preservación del valor fracasan irremediablemente. Hay una buena razón por la cual las letras de cambio eran redimibles en oro: este, gracias a su condición de buena moneda, le otorgaba estabilidad a todo el sistema. La buena moneda permite trasladar el valor no sólo en el espacio sino también en el tiempo, y así acumular el fruto de las actividades productivas para uso futuro. Esta propiedad

> es tan importante que de ella depende el funcionamiento de todo mercado extenso.

Ripple no sustituirá a Bitcoin, pero en caso de tener éxito sin duda lo complementará y lo potenciará. Al proveer nuevos canales para descentralizar los intercambios, Ripple podría acabar reemplazando algún día a los exchanges, haciendo a la economía Bitcoin independiente de los sitios que hoy resultan ser sus puntos más débiles.

II - Hacia la libertad monetaria

El escrito que inspiró a Satoshi Nakamoto

Bitcoin es la implementación de un concepto que fue ideado tiempo atrás por el criptógrafo Wei Dai, quien publicó en el año 1998 una extraña propuesta en la lista de correo electrónico *Cypherpunk*: un sistema de intercambio de valor y ejecución de contratos basado en una moneda electrónica irrastreable, que les permitiera a sus dueños mantenerse anónimos. A esta moneda la llamó "*b-money*".

La propuesta de Wei Dai no despertó en su momento mayor interés, pero más adelante – nadie sabe a ciencia cierta cuánto tiempo después – fue rescatada silenciosamente, desarrollada y perfeccionada por Satoshi Nakamoto, quien decidió incluirla como referencia en su ya célebre *paper (“Bitcoin: A Peer-to-Peer Electronic Cash System”)*, publicado en el año 2008.

He aquí un fragmento del texto que inspiró a Satoshi Nakamoto, traducido al español:

“Me fascina la idea de Tim May de una sociedad completamente voluntaria y protegida por medio de la criptografía. A diferencia del tipo de comunidad tradicionalmente asociado con la palabra “anarquía”, en una cripto-anarquía el gobierno no es eliminado, pero es incapaz de imponerse. En este tipo de comunidad, la amenaza de la violencia resulta impotente, dado que no es posible ejercer la violencia sobre miembros de una comunidad que no pueden ser identificados en contra de su voluntad.

Hasta ahora no está claro, ni siquiera en teoría, cómo podría funcionar semejante comunidad. Una comunidad se define por el nivel de cooperación entre sus miembros, y para que esa cooperación sea eficiente, es necesario contar con un medio de intercambio (dinero) y determinar la manera en que se harán cumplir los contratos. Tradicionalmente, estos servicios han sido proporcionados por los gobiernos (o por instituciones patrocinadas por los gobiernos) a personas físicas o jurídicas definidas por ellos. En este artículo describiré un protocolo en virtud del cual dichos servicios pueden ser

suministrados a entidades irrastreables y por entidades irrastreables.”

AL RESCATE DE LOS AHORRISTAS

Muchos esperan ansiosamente la irrupción del software que ponga finalmente a Bitcoin al alcance del gran público. Nosotros, en cambio, pensamos que la adopción masiva de Bitcoin dependerá más de la crisis del sistema monetario vigente que de las nuevas aplicaciones montadas sobre el protocolo ideado por Satoshi Nakamoto.

Las mejoras al *core software* y los nuevos emprendimientos en torno a Bitcoin son – y siempre serán – bienvenidos, pero la gente es capaz de aprender a lidiar con el archivo *wallet*.dat – y mucho más que eso – si es con el fin de proteger los ahorros arduamente obtenidos.

¿Acaso abrir una cuenta en el extranjero es algo sencillo y seguro para individuos de clase media o baja?; ¿acaso lo es comprar y resguardar monedas de oro; elegir un fondo de inversión; encontrar un asesor financiero confiable? … ¿y cuánto se paga por estos “privilegios” cuando el capital propio se ve amenazado?

Tal como existe hoy en día, Bitcoin ya supera ampliamente a todo lo conocido en materia de preservación del valor. El precio del bitcoin puede fluctuar en el corto plazo, sí, pero el número de bitcoins que llegarán a existir no cambiará. Cada vez se generarán menos bitcoins: esto es tan cierto como que cada vez se emitirán más dólares, euros, pesos, etc.… hasta el inevitable colapso económico.

Así que no será el amor, sino el espanto, lo que despertará el interés por Bitcoin en el gran público – ávido de alternativas a un sistema monetario agonizante.

AL RESCATE DE LA POBLACIÓN PRODUCTIVA

¿Qué pasaría si una masa crítica de la población de algún país decidiera usar bitcoins como medio de intercambio, refugio de valor y unidad de cuenta?

Tras el matemáticamente inevitable colapso financiero del "Estado benefactor", los miembros de las clases productivas no se quedarán de brazos cruzados. Pero necesitarán un sistema monetario que los proteja de la rapacidad estatal, y que sea capaz de sustentar la división del trabajo en una sociedad tecnológicamente avanzada. En otras palabras, necesitarán a Bitcoin – y lo adoptarán de muy buen grado. Este es un escenario verosímil a juicio de Michael Suede, y en tal eventualidad éstas son las consecuencias que él vaticina:

(...)

"En pocas palabras, si la gente quisiera conservar su dinero, podría hacerlo. El Estado sólo obtendría el dinero que la gente quisiera entregarle. ¿Cuánto tiempo podría sostenerse un Estado moderno si la gente usara masivamente una moneda imposible de rastrear o confiscar? Supongo que no mucho, puesto que la existencia misma del Estado depende de la coacción."

(...)

"Una región del mundo en donde Bitcoin llegara a convertirse en la moneda dominante acabaría con el control fascista de la banca moderna, y con el mismo Estado-nación – que se financia mediante la violencia. La nueva moneda digital descentralizada no podría ser contenida, ni siquiera por medio de una acción mundial coordinada de todos los Estados. No, los incentivos económicos inherentes al comercio son demasiado poderosos. La prohibición del uso de Bitcoin tendría tanto éxito como lo ha tenido la prohibición del uso de ciertas drogas."

El sistema monetario actual se nos impone con un único propósito: quitarnos parte del fruto de nuestro trabajo (dejándonos conservar lo necesario para que sigamos produciendo). Esperar que nuestros amos se den cuenta de lo injusto que es el régimen que ellos gobiernan y, en un rapto de compasión, decidan liberarnos, es tan razonable como esperar que un granjero libere a su ganado.

¿Eres partidario de las reformas?: debes saber que este sistema sólo se reforma para exprimirte mejor.

¿Quieres pruebas de que eres un esclavo?: ¡mira tus cadenas! Hace falta violencia (dinero de curso forzoso, impuestos) para hacer funcionar a un sistema injusto.

¿Pretendes respeto como individuo productivo?: ¡deja de reclamárselo a quien sostiene el látigo!

Si estamos encadenados es precisamente porque nuestros amos (y el creciente número de parásitos que de ellos dependen) saben que no hay otra forma de mantener sus privilegios. En ausencia de una población productiva esclavizada, enfrentarían un terrible dilema: ganarse la vida honestamente (¡Dios no lo permita!)… o mendigar para sobrevivir. Para ellos, mantener el *statu quo* es literalmente una cuestión de vida o muerte, pues no hay parásito sin huésped. No es de extrañar, entonces, que sea tan elevado el costo de romper las cadenas que nos sujetan… Pero eso está a punto de cambiar.

Para la población productiva, el costo de la liberación disminuye a medida que Bitcoin se expande. De modo que si tú rechazas la inmoralidad – tanto como la idea de esconderte en el bosque para evitarla – tienes ahora la oportunidad de ayudar a construir un mundo diferente.

Utiliza hoy el medio de intercambio del mañana: tu bolsillo y tu conciencia – y las futuras generaciones – te lo agradecerán.

Al rescate de las víctimas de la inflación

Tras años de constante devaluación, haz lo siguiente: reemplaza un signo monetario por otro cuya unidad equivale a miles – o, si te resulta conveniente, millones – de unidades del anterior. Repite la operación cinco veces, como ha hecho el Banco Central de la República Argentina desde el año 1935, y llegarás a tener una unidad de un valor igual a miles de trillones de unidades correspondientes al signo monetario que inició esta lamentable serie.

Quizás el de Argentina sea un ejemplo extremo, pero no es una excepción. De hecho, el promedio de vida de un signo monetario nacional es menor a los 50 años.

¿A dónde ha ido a parar todo ese ahorro, toda esa riqueza que alguna vez fue creada? – por no hablar de las deudas jamás cobradas, las rentas

devaluadas, las jubilaciones evaporadas, los proyectos truncados, las inversiones malogradas…

La inflación se lo ha comido todo, y en su lugar nos ha dejado atraso, pobreza, miseria, y una sociedad estratificada, en la cual unos reciben el dinero recién emitido y otros lo reciben ya devaluado; unos dominan los métodos para ganarle con creces a la inflación y otros apenas logran sobrevivir con un ingreso que pierde su valor mes a mes.

Los primeros constituyen la clase privilegiada (aunque no necesariamente opulenta), conectada políticamente, con acceso a la banca *off shore*, a sofisticados instrumentos financieros, a contadores y abogados enterados de las últimas regulaciones, a subsidios, a prebendas, a información interna, a créditos "blandos" costeados por el erario público – es decir a deuda que será licuada gracias a la misma inflación que otros padecen sin paliativos.

Las principales víctimas de la inflación seguirán siéndolo mientras no identifiquen el origen del problema y, por lo tanto, sigan acudiendo a sus verdugos en busca de ayuda. Por eso lo diremos otra vez, para quienes todavía no se han sacudido el relato mitológico que hoy llaman educación: el origen del problema es un sistema monetario basado en dinero de curso forzoso, y la densa maraña de leyes que le da sustento.

La próxima vez que alguien te pregunte por qué hay tanta indigencia en el mundo, explícale que la causa del aumento sistémico de precios no es el afán de lucro de los empresarios, sino el aumento discrecional de la masa monetaria. Si logras que lo entienda, ¡felicitaciones!: habrás despojado al rebaño de una oveja.

Y si alguien te pregunta cuál puede ser la solución a este problema, explícale que Bitcoin posee todas las ventajas del oro – un *commodity* que mantuvo su poder adquisitivo durante miles de años – pero ninguna de sus desventajas.

El oro jamás ha precisado, y jamás precisará, un signo monetario bendecido por un gobierno para que su valor sea aceptado, ya que su condición de buena moneda obedece exclusivamente a sus atributos. Lo mismo cabe decir de Bitcoin.

Bitcoin y la libertad financiera

Bajo el sistema de dinero de curso forzoso, estamos obligados a confiarle nuestro dinero a fondos de inversión (o bien aprender a elegir títulos negociables), a contratar asesores, abogados, contadores, gestores, y a hacer toda clase de piruetas financieras… tan sólo para aspirar a – en el mejor de los casos – conservar el poder adquisitivo que hemos ganado con sangre, sudor y lágrimas.

De no ser por la perpetua devaluación del dinero de curso forzoso… ¿cuántas personas dedicarían su precioso tiempo al estudio de aquellas inversiones que no estuvieran directamente relacionadas con su propia carrera o empresa? Toda esa energía consagrada a "ganarle" a la inflación (presente o futura) es energía robada a la clase productiva. Para el conjunto de la economía, esto significa – entre muchos otros males – desperdicio de recursos, oportunidades malogradas, productividad no alcanzada, bienes que nunca llegarán a materializarse y servicios que nunca serán prestados.

Conservar lo propio – algo tan simple, tan justo, tan necesario – se ha transformado en una ciencia oculta, en torno a la cual proliferan los expertos. Pero no necesitamos expertos; para alcanzar la prosperidad (individual y socialmente) lo único que necesitamos es que nos permitan disponer del fruto de nuestro trabajo. En definitiva, que nos dejen crear, trabajar, producir e invertir en paz. Sin embargo, para los miembros de la clase productiva (pues no hay más que dos clases: la parasitaria y la productiva) hoy en día es más fácil alcanzar la cima del Everest que la libertad financiera.

Bajo reglas abstractas, coherentes y no arbitrarias – en otras palabras, bajo reglas justas – perfeccionarse en una determinada disciplina, trabajar duro e integrarse eficientemente en un sistema de división del trabajo son factores que condicionan, salvo muy mala fortuna, el éxito económico (y aún en caso de mala fortuna, la prosperidad ajena ayuda a paliar la desgracia propia).

Bajo las reglas hoy vigentes, en cambio, es común encontrar a gente extraordinariamente noble y productiva sobreviviendo a las cambiantes regulaciones, a la corrupción, a la inflación, a los crímenes que sus impuestos no sólo no detienen sino que promueven; gente forzada a entregar el fruto de su trabajo a una clase parasitaria en expansión, y destinada a una vejez de pobreza tras haber dedicado la vida entera a la satisfacción de necesidades ajenas muy concretas.

El poder del dinero

Si no podemos entender qué es la moneda, estamos condenados a ver en ella lo que se nos antoja ver; a proyectar nuestros deseos, nuestros prejuicios o nuestros temores más profundos en algo inerte, como hacen los animistas en la selva recóndita.

Como hemos mencionado en más de una ocasión, la moneda es una herramienta utilizada para facilitar el intercambio indirecto y la preservación del valor, que sirve además como unidad de cuenta. El poder coactivo que tantos le atribuyen a la moneda no es más que una ilusión, como el poder que los misóginos le atribuyen a las mujeres, o los antisemitas a los judíos.

Quien usa dinero – por definición – está negociando. En otras palabras: si el dinero es mi única herramienta y no me he ganado tu consentimiento, no hay nada que yo pueda hacer para controlarte. A diferencia de otras herramientas, como las que usan los mafiosos para imponer su voluntad, el dinero sólo ayuda a lograr objetivos por medio de acuerdos mutuamente beneficiosos.

Con dinero no puedo quitarte nada que tú no quieras darme – algo que sí puedo hacer, por ejemplo, con una escopeta. Puedo usar dinero para comprar una escopeta, claro, pero sólo puedo obligarte a hacer algo si te apunto con mi escopeta, no con mi dinero. Con mi dinero podría intentar persuadirte, nunca forzarte.

Usar (el propio) dinero es, en definitiva, lo opuesto a usar la violencia – de hecho, es una manera de impugnar la violencia. Por eso la institución moneda es el blanco predilecto de la intervención estatal. Y por eso Bitcoin – la moneda a prueba de monopolios – hará temblar a quienes hoy, escudados tras el monopolio de la fuerza, nos exigen obediencia a punta de pistola.

Un sistema monetario a prueba de monopolios

El monopolio sobre la emisión de moneda en un determinado territorio es tan ilegítimo – y tiene efectos tan desastrosos – como el monopolio sobre la

producción de alimentos, o sobre la atención médica. Si esta afirmación es lógica, y es muy fácil de entender, y además está demostrada hasta la náusea… ¿por qué, entonces, tanta gente opina lo contrario? En gran medida, porque hay un monopolio sobre los programas educativos – que se encuentra en la raíz de todos los otros monopolios.

Hace falta una gran dosis de violencia cotidiana, especialmente dirigida a los niños más inteligentes, para enseñarles que la mejor forma de lidiar con los problemas es recurriendo a la violencia (impuestos, regulaciones arbitrarias, intimidación, castigos para los "rebeldes", etc.)

"Dadme un niño de hasta nueve años y será mío para toda la vida", decían los jesuitas. Pero tenemos malas noticias para los encargados de adoctrinar a las nuevas generaciones: Internet llegó para quedarse. Les deseamos mucha suerte intentando vender su historia oficial a un joven despabilado con acceso a la web, o explicando las bondades del dinero de curso forzoso a un joven que, sin cuenta bancaria ni tarjeta de crédito, puede enviar bitcoins a cualquier parte del mundo con la misma facilidad que envía un e-mail. Van a necesitarla.

La generación Bitcoin

La "generación Bitcoin" será la primera generación monetariamente libre. Sus miembros, a diferencia de los miembros de las generaciones previas, no se someterán al mandamás que les toque en suerte, pues ignorar los mandatos gubernamentales será tan fácil para ellos como lo es hoy para nosotros ignorar las advertencias de un hechicero.

Los miembros de la generación Bitcoin no serán siervos ni señores - ni aspirarán a serlo. Lejos de permanecer atados a una jurisdicción - condenados trabajar para sostener a una casta de parásitos y a lidiar con regulaciones impuestas por la fuerza - viajarán libremente por el mundo (virtual o real), cambiando sus bitcoins por mala moneda cuando no les quede otra alternativa. Esa será la única concesión que harán a los representantes de la fuerza bruta.

Apartándose tanto de la alienación como de la marginalidad, los miembros de la generación Bitcoin optarán por ganarse la vida sin rendir cuentas a los matones de turno, y se rehusarán a pagar las deudas de esa organización

delictiva que llaman Estado. Al fin y al cabo - se preguntarán - ¿qué les debemos a todos esos diputados, senadores, concejales, ministros, etc.?; ¿qué hacen ellos, además de quitarnos el dinero a punta de pistola, endeudarse en nuestro nombre, mandonearnos, complicarnos la vida, obstaculizar la producción y el comercio - en fin, además de entorpecer la libre interacción entre seres humanos?

A quienes integran la clase parasitaria (y a su séquito de secretarios, consultores, burócratas y camaradas prebendarios), los miembros de la generación Bitcoin les dirán: "¿Están seguros de que los necesitamos? ¡Pues entonces demuéstrenlo! Si resulta que estamos interesados en contratar sus servicios, les pagaremos con bitcoins."

ESCENAS DE LA VIDA COTIDIANA ANTES DE BITCOIN, NARRADAS EN PRIMERA PERSONA

Sus fondos han sido expropiados – ¡muchas gracias por elegirnos!

Palabras más, palabras menos, este es el cordial intercambio de emails entre un cliente del conocido procesador de pagos Dineromail y una empleada de esta empresa:

Cliente*: Hola, gracias por responder a mi consulta. Mi problema es que no veo los fondos que tenía depositados en mi cuenta. ¿Cuál puede ser el motivo?*

Dineromail*: Hola. Gracias por contactarse. El débito de su cuenta se ha realizado porque la misma estuvo en desuso más allá del lapso descripto en la cláusula 7.328, inciso decimocuarto bis [N de la R: probablemente sea el decimoquinto bis, ahora no lo recuerdo] de los términos y condiciones del servicio.*

C*: Gracias por su respuesta. ¿Es posible recuperar esos fondos de alguna manera?*

D*: Hola. Gracias por contactarse. No es posible recuperar el saldo que fue debitado de su cuenta. Este será transferido a una "cuenta general"*

antes de proceder al cierre definitivo de su cuenta si esta no registra movimientos [N de la R: en rigor, los términos y condiciones dejan claro que las cuentas "pueden cerrarse sin invocación de causa"] ¡Muchas gracias!

***C**: Sólo me queda una duda: ¿voy a recibir algún aviso antes de que procedan a cerrar mi cuenta? Gracias por su tiempo.*

***D**: Hola. Gracias por comunicarse nuevamente. No se le enviará una notificación previa al cierre de su cuenta. ¡Qué tenga buen día!*

¿Cómo es posible que un negocio funcione – y prospere – de esa manera? La respuesta se sigue de otra pregunta: ¿Qué alternativas tienen sus clientes? El problema de Dineromail no es la representante que me tocó en suerte, ni algún otro empleado, ni su fundador, ni su actual dueño. No: el problema es la escasa o nula competencia que hay en el rubro de los procesadores de pagos. En otras palabras, el problema es la existencia de un monopolio (u oligopolio), creado por regulaciones a las que sólo pueden sobrevivir los gigantes – por torpes que sean.

Me pregunto, sin embargo, si estos gigantes saben lo que les espera; me pregunto si son capaces de imaginar a un competidor que no reconoce fronteras ni privilegios. No lo creo, y no los culpo: un sistema de transferencia de valor abierto y transparente, inmune al soborno y a la amenaza, que se expande sin necesidad de contactos políticos ni departamento de marketing es, para ellos, inconcebible. Pero existe, y cuando lo vean venir será demasiado tarde.

Los procesadores de pagos montados sobre el sistema monetario estatal correrán la misma suerte que las oficinas de telégrafos, los agentes de viajes y los locales de venta de discos compactos. Da igual si lo saben o no, ya que nada pueden hacer para evitarlo: en la era de Internet, el "servicio" que brindan no tiene razón de ser. Su desaparición – o, en el mejor de los casos, su reducción a la insignificancia – será un mero efecto secundario de la expansión de Bitcoin.

Una mañana (¿perdida?) en el banco

Son las diez y media de la mañana. La larga fila de individuos que esperan su turno llega hasta la acera. Indeciso, me acerco al policía que custodia la

entrada del banco y le pregunto si toda esa gente está esperando a ser atendida en las cajas, o si algunos están ahí por otro motivo. “Todos para las cajas”.

Antes de unirme a la fila, doy un último vistazo a quienes la integran: es encabezada por un hombre de al menos ochenta años, visiblemente cansado – lleva más de media hora defendiendo su lugar en la fila. No tiene donde sentarse. Abundan los jubilados y las amas de casa; un joven mira su reloj y abandona la fila.

Nadie sabe por qué todavía no han empezado a atender al público – es que nadie lo ha explicado. Antes de unirse a la fila, cada nuevo integrante hace la pregunta de rigor: “¿Toda esta gente está para las cajas?”. Parece que en el curso de treinta años a nadie se le ha ocurrido pegar un cartel que diga: “Cajas: fila aquí”.

A las once de la mañana empiezan a circular algunos rumores: “No llegó el tesorero”, “Llegó el tesorero pero no hay sistema”, “Hay sistema pero no hay efectivo”… Le pregunto a una señora que habla en voz alta cuál de todos los rumores le parece más verosímil. “No sé, pero no creo que vayan a atender hoy”, me dice. Sin embargo, no se mueve de su lugar en la fila.

¡Aleluya! Siendo las once y cuarenta y cinco de la mañana, la fila empieza a moverse. Lo hace lentamente, ya que de las tres cajas una sola está abierta. Me alegro por el anciano que llevaba dos horas esperando su turno. Ruido de sellos, impresoras, teléfonos que suenan. Hay un único empleado en el mostrador; todos los demás están ocupados completando formularios y llevando papeles de aquí para allá.

¡Mi turno! Son las doce y cuarenta del mediodía. El empleado me habla pero no me mira. Con voz monocorde me interroga: “nombre, apellido, documento de identidad, número fiscal…” Hago mi depósito y huyo, con la sensación de haber visitado un museo que las generaciones futuras mirarán con asombro, y feliz de haber usado este sistema moribundo para comprar bitcoins.

Feliz digo, a pesar de todo, porque el valor de cada bitcoin adquirido es independiente de los caprichos gubernamentales, y porque al cambiar dinero de curso forzoso por moneda libre contribuyo a debilitar una institución violenta, corrupta y obsoleta que está destinada a caer… y merece caer.

CUARTA PARTE

MERCADO

I - Bitcoin como inversión

El precio y el valor fundamental

Antes de invertir… ¿en qué se fija el buen inversor? En el valor fundamental de aquello que le interesa.

En el caso de Bitcoin, esto significa: número de comerciantes que aceptan bitcoins como medio de pago; nuevos emprendimientos y aplicaciones en torno a Bitcoin; desarrollo del ***core software*** de Bitcoin; garantía de posesión de los propios bitcoins (inviolabilidad de la cadena de bloques); adelantos en la protección de las "billeteras" Bitcoin; ventajas de Bitcoin respecto a otras monedas; riesgo de que el sistema sea eliminado; potencial de Bitcoin…

Luego de fijarse en el valor fundamental, el buen inversor echa un vistazo al precio. ¿Hay una diferencia significativa entre éste y aquél? Su decisión final dependerá de la respuesta a esa pregunta.

Una vez tomada la decisión, el buen inversor ya no mirará hacia atrás, ni se inmutará por los comentarios de quienes no se han molestado en hacer su propio análisis.

Más allá de las creencias y los estados anímicos predominantes en cada momento, Bitcoin seguirá funcionando de acuerdo a las reglas que fija su protocolo.

Por qué subió el precio del bitcoin

El 1º de Enero del año 2011, el bitcoin cotizaba a US$ 0,30. El 1º de Enero de 2012 – exactamente un año después – el precio de un bitcoin alcanzó los US$ 5,50. Esto es, un incremento del 1.833% (sí, mil ochocientos treinta y tres por ciento) en sólo un año. En Enero de 2013, el precio de un Bitcoin supera los US$ 20. Nada mal para un proyecto que tantos "expertos" han dado por muerto.

Pero si este rendimiento les parece formidable (y lo es, comparado con el

de casi cualquier otra inversión) es porque no han tenido en cuenta que se ha dado a pesar de una expansión monetaria cercana al 40% anual (es decir, a pesar del máximo nivel de inflación de la base monetaria que es posible en el marco del protocolo de Bitcoin). En Noviembre del año 2012, el incremento de la masa monetaria se redujo bruscamente a la mitad – evento que se repetirá indefinidamente cada 4 años.

Las explicaciones coyunturales de la cotización del bitcoin en determinados momentos del año – especialmente durante las grandes oscilaciones – varían considerablemente, pero no deberían distraernos; al fin y al cabo, todas ellas pasarán a la historia como meras curiosidades en el museo de la especulación.

La explicación de fondo, en cambio, es sencilla para cualquiera que esté familiarizado con los principios básicos de la ciencia económica. En palabras de Michael Suede:

"Recuerden que es el mercado el que nos dice qué es moneda y qué no lo es. Y el mercado ha hablado. Los bitcoins tienen valor porque el mercado dice que tienen valor. No se imponen por decreto gubernamental. No hay leyes que nos obliguen a usarlos. Tienen valor simplemente porque la gente aprecia las ventajas inherentes a un sistema de intercambio digital descentralizado e inmune a la manipulación arbitraria de una institución vertical.

Bitcoin es fruto del libre mercado; es la moneda de la era digital. Bitcoin es la solución al problema de la inflación de los recibos de oro por parte de bancos y gobiernos (algo que siempre acaba ocurriendo bajo el patrón oro). Bitcoin es la solución a los problemas de fraude que impregnan a todos los sistemas de intercambio basados en meras representaciones en papel – o digitales – de commodities."

II - Algunos emprendimientos

BitPay obtiene fondos por US$ 510.000

El mayor procesador de pagos con bitcoins ha completado una ronda de financiación por 510.000 dólares. Entre otros, han participado en la misma Barry Silbert (el fundador de SecondMarket), Shakil Khan (uno de los primeros en invertir en Spotify), Jimmy Furland y Roger Ver.

WordPress enciende la mecha de Bitcoin

A juzgar por el anuncio de WordPress – la compañía líder en servicios de publicación en línea –, la decisión de empezar a aceptar bitcoins ha sido tomada por muy buenas razones:

“Si bien aquí [en WordPress.com] cualquier persona puede empezar un blog de manera gratuita, no todos pueden acceder a nuestros servicios de mejoras debido a los límites impuestos por las redes de pago tradicionales.

Pero eso está a punto de cambiar: ahora se pueden adquirir los productos de WordPress.com con bitcoins.

PayPal, por ejemplo, bloquea el acceso desde más de 60 países, y muchas compañías de tarjetas de crédito tienen políticas similares. Cualquiera sea la razón, no creemos que un blogger de Haití, Etiopía o Kenia deba tener menos acceso a la blogósfera por cuestiones que escapan totalmente a su control.

A diferencia de PayPal y las tarjetas de crédito, Bitcoin no tiene autoridad central ni manera de dejar a países enteros fuera de la red. El comerciante que acepta pagos por medio de Bitcoin puede hacer negocios con quienquiera, esté donde esté él o su contraparte.”

GoldMoney se acerca a Bitcoin

En un giro que hasta los bitcoiners más optimistas hubieran considerado improbable, GoldMoney ha empezado a estudiar la posibilidad de integrar a Bitcoin a su sistema. GoldMoney es una prestigiosa compañía que ofrece servicios de compra, venta y almacenamiento de metales preciosos en jurisdicciones "seguras", actualmente a cargo de unos dos mil millones de dólares en metales preciosos – propiedad de los más de 23.000 clientes que tiene en todo el mundo.

TorrentLeech, el conocido torrent tracker, acepta bitcoins

TorrentLeech no es el primer tracker privado en aceptar bitcoins, pero sí el más grande: hoy cuenta con más de 500 mil usuarios, y una trayectoria de 8 años en el rubro.

Del anuncio en el foro de Bitcoin:

"Como algunos de ustedes ya habrán notado, hemos comenzado a aceptar donaciones en bitcoins. Estamos convencidos de que es la mejor manera de realizar pagos, ya que con Bitcoin es posible proteger el anonimato de los usuarios.

Somos concientes de las ventajas de Bitcoin, y es por eso que hemos decidido que aquellos que realicen sus pagos con bitcoins recibirán meses adicionales de acceso VIP."

De la página wiki de TorrentLeech:

"Siendo esta una comunidad p2p, es importante para nosotros aprovechar y apoyar otros proyectos p2p que expresan los mismos ideales que nuestra comunidad.

Bitcoin lleva unos años entre nosotros, y puede considerarse una moneda probada. Creemos que ha llegado para quedarse, y que ya puede usarse en

forma segura para realizar transacciones cotidianamente."

CoinDL: el iTunes del mundo Bitcoin

Presentación del proyecto en el foro de Bitcoin:

"Al hacer un balance de la enorme cantidad de herramientas que los bitcoiners han desarrollado, queda claro que Bitcoin ya está listo para ser la base de una nueva economía.

Es hora de que las personas empiecen a ganar bitcoins de la misma forma en que ganan dólares, euros o yenes. Ahora podrán hacerlo por medio de un sistema con el cual muchos ya están familiarizados: el mercado de descargas digitales.

CoinDL *cuenta con un proceso de compra muy fácil de usar. Micropagos; transacciones rápidas y sin riesgo para la privacidad; interfaz limpia y amigable – todo lo necesario para aplacar al geek más salvaje."*

Premiumize.me: proxy anónimo a cambio de bitcoins

Al aceptar bitcoins como medio de pago, ***Premiumize.me*** se une a los numerosos servidores proxy que ahora ofrecen esta nueva capa de anonimato – especialmente necesaria para aquellos usuarios que viven bajo el yugo de gobiernos totalitarios.

CoinWorker, o cómo ganar bitcoins usando tu mente

Trabajar online a cambio de bitcoins nunca ha sido tan fácil, gracias al Mturk del mundo Bitcoin: *Coinworker*.com.

YCombinator ha financiado un emprendimiento relacionado con Bitcoin.

Coinbase, un emprendimiento que apunta a ser el Paypal de Bitcoin, ha recibido financiamiento de *YCombinator*, la mayor incubadora tecnológica del mundo.

Ogrr.com: el Western Union de los bienes virtuales

El extraordinario crecimiento de ***Ogrr.com*** se puede atribuir al hecho de que Bitcoin es, por lejos, la manera más eficiente y barata de mover la riqueza obtenida en mundos virtuales (entre diferentes mundos virtuales, o bien de un mundo virtual al mundo real).

Diaspora se financia con bitcoins

La red social que aspira a competir con *Facebook* haciendo hincapié en la privacidad, ha empezado a recibir donaciones en bitcoins.

Okpay.com acepta depósitos en bitcoins

Okpay.com, uno de los principales procesadores de pagos online (300.000 cuentas funcionando en Marzo de 2011), acepta depósitos en bitcoins.

Con blockchain.info pueden hacerse transacciones de múltiples firmas

El software ideado por Satoshi Nakamoto tiene el potencial de admitir toda clase de transacciones complejas, es decir transacciones que involucren a más de dos partes, y que se lleven a cabo según reglas y condiciones libremente acordadas.

La gente de *blockchain.info* ha implementado el primer servicio de depósitos en custodia que no depende de un mecanismo centralizado para funcionar (sino de la sempiterna cadena de bloques). Cabe destacar que

además de ser descentralizado, este servicio es anónimo – y extraordinariamente barato comparado con las alternativas disponibles. Así lo describen sus creadores:

“Normalmente, los bitcoins se envían a una dirección Bitcoin única, y quien posea la clave privada correspondiente a dicha dirección tendrá el poder de gastar esos fondos. Con las transacciones de múltiples firmas, pueden incluirse hasta 3 direcciones diferentes (las de los eventuales destinatarios). Para que se liberen los fondos “en custodia” se requiere la aprobación de un número previamente acordado de aquellos destinatarios.

Ejemplo: Los fondos correspondientes a una transacción entre Alice (cliente) y Bob (comerciante) quedan “en custodia” hasta que Bob cumple con la obligación que ha contraído con Alice. Si Bob y Alice no logran ponerse de acuerdo, pueden recurrir a los servicios de una tercera parte (el árbitro) para que decida cuál debe ser el resultado de la transacción.”

Bitcoin Card: el futuro del futuro de la moneda

Bitcoin Card es una increíble pieza de tecnología que combina la creación de redes, el autoabastecimiento de energía y la informática súper delgada. Se espera que actúe como una plataforma segura para almacenar bitcoins y efectuar transacciones.

Wikispeed: el primer fabricante de automóviles en aceptar bitcoins

WIKISPEED aplica los principios del desarrollo de software libre a la fabricación de automóviles, logrando resultados extraordinarios en el diseño de prototipos de alta eficiencia y alto rendimiento.

El carácter descentralizado y abierto de Bitcoin resuena profundamente en la esencia del proyecto WIKISPEED. Por primera vez en la historia, es posible comprar un coche fabricado por una empresa colaborativa y descentralizada, usando una moneda que no ha sido emitida por ningún banco.

Dragon's Tale: el primer MMORPG basado en Bitcoin

De esta manera lo presentó su creador en el foro de bitcoin:

"¿Qué tal si hubiera un tipo de casino diferente a todos los casinos conocidos, que existiera en un "mundo virtual persistente"? – un mundo en el que todo lo que ves y todo lo que tocas es, de hecho, alguna clase de juego. Sin máquinas tragamonedas tradicionales, sin juegos de cartas o dados, sino un juego de rol en el que tu personaje avanza a medida que tiene éxito en los distintos juegos.

Bitcoin ha reavivado esa idea en mí. Desde que conocí a Bitcoin he estado imaginando ese mundo. En septiembre [de 2010] he empezado a programar **Dragon's Tale***, un MMORPG que usa bitcoins exclusivamente. El juego está construido bajo el sistema eGenesis I, el mismo cliente/servidor que usa* **A Tale in the Desert***."*

FarmVille le abre la tranquera a Bitcoin

FarmVille es un videojuego en tiempo real desarrollado por *Zynga*, que permite manejar una granja virtual desde la plataforma de *Facebook* (y a través de una aplicación para *iPhone*). Poco después de su lanzamiento en Junio de 2009, *FarmVille* se convirtió en el juego más popular entre los miembros de *Facebook*, superando los 80 millones de usuarios activos mensuales.

Y bien, los responsables del sitio oficial de *FarmVille* (el cual recibe más de 100.000 *clicks* diarios) han decidido promover el uso de Bitcoin y empezar a aceptar publicidad a cambio de bitcoins. Ellos mismos explican por qué:

"Al colocar avisos por los cuales los anunciantes están dispuestos a pagar con bitcoins, estaremos ahorrándonos las comisiones que nos cobran los servicios tradicionales. Por tal motivo, le daremos prioridad a los avisos pagados con bitcoins."

Bitcoin parece estar haciéndose más y más popular cada día, y es fácil entender por qué."

A la conquista del mercado de apuestas online

Son muchos los sitios web que ofrecen apuestas con bitcoins. Esto es lo que respondió el gerente de BTCSportsBet.com cuando se le preguntó por qué Bitcoin es preferible a otros medios de pago:

"Como usted sabe, la transferencia de dinero es vital para la industria de las apuestas online (deportivas, casino, póker online, etc). Bitcoin es una solución increíble.

(...)

Parte del valor de Bitcoin reside en su utilidad. Uno puede enviar bitcoins a cualquier usuario en cualquier lugar de mundo, prácticamente sin costo. Y rápidamente: las transacciones son verificadas por la red en cuestión de minutos, y se procesan de forma automática. BTCSportsBet.com maneja docenas de este tipo de transacciones al día (depósitos y retiros) sin intervención humana. Esto es increíblemente eficiente, tanto para el sitio como para los jugadores, quienes pueden depositar en la mañana, apostar en un juego, ganar, y retirar los fondos inmediatamente después del juego. Más tarde pueden apostar en otros juegos, y luego volver a retirar los fondos, todo rápidamente y sin comisiones – y lo más importante, sin tener que lidiar con bancos, ni compañías de tarjetas de crédito, ni Western Union, ni PayPal, ni cualquier otro intermediario. ¿Qué otro sistema permite un procesamiento tan eficiente de las transacciones?

Y una vez que los bitcoins son enviados, la transacción no puede ser revertida sin el consentimiento del receptor – a diferencia de lo que ocurre a menudo con las tarjetas de crédito. ¿Qué comerciante, vendedor o corredor de apuestas no prefiere un sistema de pago irreversible, y por lo tanto inmune al fraude? Desde el punto de vista del usuario, el problema del robo de identidad queda solucionado, ya que no es obligatorio revelar datos personales."

QUINTA PARTE

MITOS Y PREGUNTAS FRECUENTES

I – Mitos

“Los gobiernos acabarán con Bitcoin”

De cuando en cuando, alguien siente la necesidad de arrojar este comentario, cual bomba Molotov, en el medio de un foro: “Tarde o temprano, los gobiernos acabarán con Bitcoin”.

Y como nuestra misión en este planeta es demostrar que hay un antes y un después de Bitcoin, hemos decidido compilar todas las razones por las cuales pensamos que los gobiernos NO acabarán con Bitcoin.

1. Es bastante fácil disimular el protocolo por medio del cual se comunican los equipos de la red Bitcoin. Algunos programas de p2p ya lo hacen y parece que funciona bien.

2. La cantidad de datos que tienen que intercambiar los equipos para mantener operativa la red Bitcoin es sorprendentemente baja. Si ofuscamos o encriptamos la comunicación entre equipos, la labor de rastreo que tendrían que hacer las operadoras de telecomunicaciones para bloquear el tráfico de Bitcoin equivaldría a buscar una aguja en un pajar.

3. El bloqueo de Bitcoin sería inútil si tan sólo un único país decidiera legalizar el protocolo. Supongamos que Suecia no lo prohíbe; para utilizar Bitcoin simplemente habría que contratar un VPN sueco.

4. Los gobiernos han luchado contra el mp3, contra PGP, contra BitTorrent… pero no se puede luchar contra los bits: las leyes que bloquean el acceso a la información no han servido para nada. Un gobierno puede conseguir, con tiempo y esfuerzo, doblegar una compañía (tipo Napster o Megaupload), pero el intercambio “no autorizado” de archivos a través de Internet no sólo no se ha reducido, sino que aumenta constantemente. De hecho, el intercambio es ahora órdenes de magnitud mayor que cuando existía Napster.

5. Bitcoin es una red descentralizada. Su arquitectura se parece mucho a la que sentó las bases de Internet, vale decir que está diseñada específicamente para eludir el daño en cualquiera de sus nodos.

6. Si Bitcoin funciona en China (y ya lo hace), puede funcionar en cualquier parte pese al esfuerzo de un Estado para censurar y controlar el flujo de información. Sólo hace falta un usuario que actúe de ***bridge*** (puente) con el exterior – una comunicación telefónica o radiofónica – y los esfuerzos de censura se ven anulados.

7. Ahora la comunicación es global, y sería un auténtico suicidio económico el suspender las telecomunicaciones de un país para que Bitcoin no prospere.

8. Los gobiernos colaboran, pero también compiten entre sí. Si se descubre que perturbar el funcionamiento de Bitcoin tiende a debilitar económicamente a una región, no van a faltar las jurisdicciones amigables para con Bitcoin.

9. La mitad de la población mundial vive en ciudades. Esto significa que, con relativamente poco desembolso per cápita, pueden formarse redes privadas ***wireless*** de transmisión de información que den soporte Bitcoin sin tener que pasar a través de los operadores de telecomunicaciones.

10. Los gobiernos están integrados por individuos, cada uno de los cuales tiene sus propios intereses. Cuando los más inteligentes entre los funcionarios de alto rango entiendan que Bitcoin es tan incontrolable como BitTorrent, empezarán a comprar bitcoins a más no poder. De hecho, puede que algunos ya lo estén haciendo.

11. Al intervenir, el gobierno estaría llamando la atención sobre Bitcoin, y reconociendo que es moneda. De esa manera, probablemente estaría acelerando – en lugar de desalentando – la adopción de Bitcoin.

12. Si los gobiernos obligaran a los bitcoiners a sumergirse en el mercado informal, estarían alimentando a una economía gigantesca (la segunda mayor del mundo después de los Estados Unidos) y en constante expansión que no paga impuestos ni licencias, y que no cumple con regulaciones gubernamentales. Basta que una mínima fracción de dicho mercado se vuelque al uso de Bitcoin para que el precio alcance niveles inimaginables hoy en día. Esto, a su vez, despertaría el interés de muchos más, tentándolos con la apreciación y las enormes ventajas competitivas que supone Bitcoin.

13. Los gobiernos necesitan a la denominada economía informal tanto o más que la población productiva. Si no fuera por la "economía informal", los funcionarios públicos no podrían vehiculizar el dinero procedente de sobornos, retornos, chantajes, dádivas y todo lo que hace a su actividad tan lucrativa. Lamentablemente para ellos, Bitcoin es inmune a la actividad política más lucrativa de todas: la manipulación monetaria.

14. Actuando en contra de los sitios de intercambio, los gobiernos llamarían la atención sobre Bitcoin, y eliminarían el único punto de entrada a la red que en cierta medida pueden controlar. Además, de esa manera incentivarían la descentralización del intercambio bidireccional entre las diferentes divisas y Bitcoin, convirtiendo así a los exchanges en intermediarios prescindibles.

15. Cabe argumentar que la crisis económica global recién está comenzando. En este contexto, Bitcoin es y seguirá siendo un hueso particularmente duro de roer, pues minimiza el costo de proteger la privacidad a la vez que hace extremadamente costoso el violar la privacidad. (Nota: con o sin crisis económica, los recursos estatales no son ilimitados).

16. La gente empieza a estar harta de que le roben vía inflación, de la manipulación de los tipos de interés por parte de los bancos centrales, de los corralitos, de los corralones, de las comisiones bancarias, de los bloqueos de cuentas, de la continua fiscalización de sus ahorros, de los "***quantitative easings***", de las dobles imposiciones en la tributación, de la reserva fraccionaria sólo para los bancos, del control en el envío de remesas, de que el tesoro venda tungsteno a precio de oro, de la prohibición de acceso al mercado de divisas… ¿Hace falta seguir?

"Cualquier multimillonario podría comprar la mayoría de los bitcoins y luego dedicarse a manipular eternamente al mercado"

Con el perdón de los creyentes, nos tomaremos el atrevimiento de revisar este artículo de fe.

Los bitcoins – a diferencia del dinero estatal – no pueden ser repartidos arbitrariamente. El que quiera pisar fuerte en el mundo Bitcoin, tendrá que

adquirirlos – a cambio de divisa u otros bienes o servicios – a precio de mercado. ¿Y qué ocurriría si alguien intentara hacerse, digamos, de varios millones de bitcoins?

En primer lugar, **dado que el número de bitcoins es limitado, su precio aumentaría bruscamente**. Esto enriquecería a los tenedores de bitcoins, cuyas expectativas – y órdenes de venta – cambiarían de inmediato, y entre los no-bitcoiners desencadenaría una masiva "fiebre del bitcoin".

Con unos cuantos millones de dólares alguien podría comprar muchos bitcoins, pero NO una elevada proporción de los bitcoins disponibles. Primero, porque **la mayoría de los bitcoins ni siquiera están a la venta** (los que se negocian son una fracción mínima del total), y segundo porque – al condicionar a la oferta – cada vez le resultarían más caros.

¿Y si los comprara por fuera de los *exchanges* (sitios de *trading*)? Secaría el mercado en minutos. Además, muchos de los que venden por fuera compran sus bitcoins en los *exchanges*, y absolutamente todos toman como referencia los precios de los *exchanges*. Así que al comprar una gran cantidad de bitcoins *over the counter*, el multimillonario afectaría inmediatamente a los precios en Mt Gox y compañía.

Si Warren Buffett decidiera invertir buena parte de su fortuna en bitcoins, el primer bitcoin le costaría unos USD 20 (al precio actual), pero el último le costaría probablemente millones de dólares – si es que para entonces tiene la suerte de encontrar a alguien dispuesto a vendérselo.

Ahora bien, supongamos que un magnate – o un gobierno – logra adquirir de alguna manera un porcentaje significativo de todos los bitcoins que hay a la fecha. ¿Qué poder le otorgaría eso?, ¿el de venderlos en un instante para deprimir el precio transitoriamente, después de haber pagado millones o billones de dólares con el fin adquirirlos? ¿Cuántas veces podría hacer algo así antes de perder todo su "poder de fuego" a manos de cada vez más compradores de oportunidad? ¿Y todo eso para qué?…

Lo único que lograría el autor de un "ataque de fuerza bruta monetaria" es despertar el interés de toda clase de inversores, que pasarían a competir con él por un activo en rápida apreciación. Y con el *dumping* ocasional sólo generaría nuevas oportunidades para los que

habían "perdido el tren". Es decir que, lejos de concentrar la distribución de los bitcoins, la estaría expandiendo.

En el caso de Bitcoin, no hay mejor manera de dispersar el mercado que tratar de dominarlo.

"Bitcoin se autodestruirá en una espiral deflacionaria"

"Dinero de curso legal" no es más que un eufemismo para referirse al dinero que nos obligan a utilizar. El estado de permanente inflación al que nos tienen acostumbrados los gobiernos es un mal innecesario, y como tal no puede sostenerse sin apelar a la violencia – porque nadie aceptaría de buen grado un dinero que tiende a depreciarse, deteriorando el poder adquisitivo y la capacidad de ahorro.

¿Y qué solución ofrece Bitcoin a este problema inmemorial? (Nótese que hablamos de "ofrecer" soluciones, que los usuarios pueden aceptar o rechazar; no de "imponer" soluciones). Algo muy simple: un límite infranqueable a la emisión monetaria. Guste o no a los gobiernos, nunca serán "emitidos" más de 21 millones de bitcoins.

Así como al pez le cuesta imaginar un mundo fuera del agua, a nosotros nos cuesta imaginar un mundo libre de inflación: un mundo en el cual no tengamos que gastar o invertir nuestro dinero sólo para evitar su depreciación, sino que, por el contrario, nos veamos incentivados a gastarlo en los productos y servicios que realmente necesitemos.

Debido a una mezcla de inercia y adoctrinamiento precoz, nos cuesta imaginar un sistema económico basado en una "moneda deflacionaria", que nos premie por ahorrar y por gastar de manera racional, promoviendo así la capacidad de invertir en proyectos de más largo plazo – proyectos que beneficiarán incluso a quienes no tienen propensión al ahorro. Por idénticas razones, nos cuesta imaginar un sistema económico basado en una moneda que ningún gobierno pueda llegar a controlar para sobre-endeudarse, gracias a lo cual el ciclo económico pase a ser un vestigio del pasado, y la guerra un proyecto inviable.

¿Y la espiral deflacionaria?… es un mito – como el unicornio, o más

precisamente: como el cuco. Lo que algunos economistas llaman “espiral deflacionaria” (la caída inesperada y sistémica de precios) en realidad tiene lugar durante la necesaria etapa de reubicación de los recursos que suele atravesar una economía (si el Estado no interfiere) tras un colapso financiero. ¿Y el colapso financiero?… es el fruto amargo de la mala inversión generalizada, inducida por años de inflación crediticia. En otras palabras, la espiral deflacionaria no es una espiral, sino un fenómeno auto-limitado que repara los efectos de la intervención estatal. (Ver “Teoría austríaca del ciclo económico”)

Está bien, pero… ¿quién gastaría un dinero cuyo valor se incrementa con el paso del tiempo, en lugar de atesorarlo indefinidamente? Respuesta: quien en un determinado momento valore lo que puede adquirirse con ese dinero… más que al dinero mismo.

Un buen ejemplo de esto es el de la tecnología informática: la gente sigue comprando computadoras, aún sabiendo que, en un futuro cercano, las computadoras tendrán más memoria, y baterías más duraderas, y serán más rápidas, portátiles, amigables… y baratas – es decir que por el mismo dinero se podrán comprar algo muy superior.

La actual renuencia a gastar los bitcoins adquiridos no es un problema; por el contrario, es testimonio de sus excelentes cualidades monetarias (la gente prefiere desprenderse de la mala moneda), y de la confianza en su valor futuro.

“Cuanto más eficiente sea la minería, más bajo será el precio del bitcoin”

El arribo de tecnologías que prometen llevar la minería de bitcoins a otro nivel ha despertado temores en algunos miembros de la comunidad bitcoiner. Y es comprensible, pues estamos moviéndonos a gran velocidad en un territorio inexplorado.

La misma palabra “minería”, en relación a una moneda digital, nos hubiera sonado poco menos que a delirio tan sólo cuatro años atrás. Pero a falta de un mapa detallado del territorio, contamos con una brújula. Nuestra brújula es la ciencia monetaria, y a ella nos aferraremos para distinguir – en la medida de lo posible – lo verdadero de lo falso.

En primer lugar, el precio del bitcoin depende tanto de la minería de bitcoins como el precio del oro de la minería de oro: esto es, muy poco. El precio del oro no se multiplicó casi por diez en el curso de diez años por un aumento de la dificultad para extraer oro, sino por un aumento de la demanda de oro como activo refugio. Y viceversa, el precio del oro no había caído antes por una disminución de la dificultad para extraerlo.

Lo que mueve el precio no es la dificultad o facilidad para obtener bitcoins por medio de minería, sino la demanda de bitcoins. Ocurre que el incentivo para minar (y por ende el poder computacional aportado a la red) suele seguir al precio, de ahí que pueda confundirse la relación causal entre dificultad y precio. Pero es importante distinguir cuál de los dos es el motor.

Por otra parte, los mineros progresan más o menos todos juntos: de CPU a GPU, de GPU a FPGA, de FPGA a ASIC. Así que la minería puede ser más eficiente en conjunto (o bien al considerar a cada minero aislado), pero **la eficiencia de cada minero en relación a los demás no mejora con la innovación tecnológica**. Minar con ASICs va a ser más eficiente, sí, pero va a serlo en la misma medida para todos los que minen con ASICs.

Por último, hay que tener en cuenta que hemos pasado la primera disminución a la mitad del premio en bitcoins por bloque hallado – un evento que se repetirá cada 4 años. En otras palabras: cada vez se distribuirán menos bitcoins entre los mineros. Y aunque esto no necesariamente condiciona el precio futuro, es una de las razones por las cuales la gente se acerca (¡demanda!) a Bitcoin: utilidad y escasez asegurada.

"Cualquiera podría hacer una copia de Bitcoin que logre desplazarlo"

Los que esto afirman tienden a ver en el código abierto una debilidad más que una fortaleza. Como el código puede copiarse, razonan, cualquiera podría usarlo para su propio beneficio. Lo que no comprenden es que las ventajas de Bitcoin no dependen en lo más mínimo del secretismo; por el contrario, **la extraordinaria vitalidad y robustez del proyecto Bitcoin son frutos de la apertura y la transparencia que constituyen su signo distintivo**.

En primer lugar, cabe recordar que las "monedas" generadas bajo las reglas

de un protocolo semejante al de Bitcoin (las “pedrocoins”, digamos, si el aspirante a fundador de la nueva criptomoneda se llamara Pedro), serían automáticamente rechazadas por los usuarios de Bitcoin. “¿Pero quién necesita a los bitcoiners?”, dirá Pedro: “Pedrocoin es el futuro; ¡viva Pedrocoin!…”

Mientras dejamos que Pedro se calme, veamos cuáles son las razones por las cuales Pedrocoin correría la misma suerte que le ha tocado en su momento a Ixcoin, a I0coin y a Freicoin, entre otros forks de Bitcoin:

First mover advantage (la ventaja del pionero)

Aunque en modo alguno garantiza el éxito frente a la competencia, ser el primero en un determinado campo implica una enorme ventaja. Es cierto que si el pionero se estanca, en algún momento será superado, pero también es cierto que el proyecto Bitcoin es inverosímilmente dinámico, y nada indica que vaya a dejar de serlo.

Network effect (efecto de red)

La moneda es la clase de instrumento que resulta tanto más útil cuantas más personas deciden adoptarlo. En su mayoría, quienes eligen a Bitcoin NO lo hacen porque aprecian la exquisita belleza de su código (aunque de seguro esto no les molesta), sino porque muchos otros lo han elegido antes.

Poder computacional

Aunque el código de Pedrocoin sea casi igual al de Bitcoin, la seguridad del sistema dependerá del poder computacional que aporten los mineros a la red – y estos no invierten en electricidad y equipos de última generación con fines precisamente caritativos. Sin el apoyo de una masa crítica de mineros bien incentivados, ningún proyecto semejante a Bitcoin tendrá la más remota posibilidad de despegar.

Ecosistema

La gente siempre tenderá a preferir, entre dos monedas, a la más líquida, vale decir a la que más fácilmente puede ser intercambiada, en todo momento, por cualquier activo. Por eso, ni siquiera una cantidad de ventajas técnicas respecto a Bitcoin serían suficientes para superar el peso de su amplia aceptación y de todo lo que a su alrededor se ha desplegado (el vasto y

complejo ecosistema de programadores, comerciantes, consumidores, emprendedores, mineros, operadores, ahorristas, etc.).

Confianza

Muchos de los que se acercan a Bitcoin en realidad están huyendo de sistemas monetarios que demandan su confianza ciega en tal o cual institución humana. Entre la promesa de un gobierno y la certeza de las matemáticas, ellos eligen lo segundo, y por lo tanto rechazarán todas las variantes de "gobiernocoins" (inflacoin, deudacoin, defaultcoin, etc) que se les presenten, digan lo que digan las autoridades. Como hemos argumentado antes, no será el amor sino el espanto lo que despertará el interés por Bitcoin en el gran público.

Comodidad

Usar simultáneamente bitcoins y pedrocoins implicaría una nueva serie de dificultades para la mayoría de los que recién están empezando a entender el funcionamiento de Bitcoin, y a gestionar sus carteras.

"En el futuro, la seguridad de Bitcoin será vulnerada por nuevas tecnologías"

El riesgo de que una nueva tecnología sea capaz de comprometer la seguridad del sistema no debería incumbir exclusivamente a los usuarios de Bitcoin: **todos los bancos – y casi todas las instituciones financieras – dependen de la criptografía para garantizar la legitimidad de las transacciones** que procesan.

¿Es posible entonces proteger a un sistema monetario digital en el largo plazo? Dado que Satoshi Nakamoto no contesta nuestros emails, hemos acudido a otro experto en criptografía para responder a esta pregunta. Como verán, si hay algo de lo cual no puede acusarse a Satoshi Nakamoto es de improvisado.

¿Qué pasaría si las primitivas criptográficas empleadas por Bitcoin (SHA-256, RIPEMD-160 o ECDSA) se tornaran "criptográficamente débiles"?

Si se volvieran lo suficientemente débiles, podrían habilitar ataques a las

claves privadas a un ritmo más rápido que mediante fuerza bruta. Así pues, las direcciones existentes pasarían a ser vulnerables (al menos en teoría). Sin embargo, Bitcoin ha sido diseñado para eventualmente ser modificado: ***el protocolo es capaz de admitir, en el futuro, la creación de direcciones basadas en nuevas primitivas criptográficas****.*

El tiempo que lleva encontrar vulnerabilidades criptográficas y aprovecharlas (si es que alguna vez llegan a ser aprovechadas) tiende a medirse en años, de modo que aún en el peor de los casos habría tiempo de sobra para difundir una nueva versión del cliente Bitcoin que les permitiera a los usuarios transferir sus monedas de las direcciones antiguas – potencialmente vulnerables – a las nuevas direcciones.

Dicho esto, es importante comprender que, ***aún en el caso de que pasáramos a un nuevo algoritmo como medida de precaución, en la práctica podría nunca llegar a utilizarse la vulnerabilidad del algoritmo anterior****.*

Les daré un ejemplo: se ha descubierto una vulnerabilidad en SHA-1 que permite un ataque de precolisión 10.000 veces más rápido que la fuerza bruta. Suena terrible, ¿verdad? En realidad no lo es. La presencia de dicha vulnerabilidad en SHA-256 (actualmente usado en minería Bitcoin) significaría que habría una probabilidad del 1% de atacar a una clave privada en los próximos mil millones de años (en lugar de una probablilidad del 0,00001%). Aún así, en ese caso sería prudente actualizar el protocolo para que admita nuevos tipos de direcciones (no tanto por la hipotética vulnerabilidad recién mencionada sino pensando en futuros hallazgos de vulnerabilidades más serias).

II - Preguntas Frecuentes

El concepto de **dinero peer-to-peer** choca con muchos de nuestros preconceptos. Estas son las respuestas a algunas de las preguntas más comunes entre quienes empiezan a adentrarse en el mundo de Bitcoin.

¿Cómo funciona una billetera o cartera Bitcoin?

El cliente Bitcoin te genera automáticamente una billetera que contiene pares de direcciones públicas y sus correspondientes llaves privadas. Las direcciones públicas son las que se ven – las que puedes dar a conocer para recibir pagos. Las llaves privadas, en cambio, sólo están en tu billetera (en el archivo wallet.dat).

Imagina que tus direcciones públicas son buzones inviolables que todos pueden ver, y en los que todos pueden depositar bitcoins, pero que sólo tú puedes abrir con tus llave privadas. Cada dirección pública se "abre" con una llave privada específica e imposible de reproducir. Si recibes 1 bitcoin que fue enviado a una de tus direcciones públicas, la única forma de eventualmente transferir la posesión de ese bitcoin (de "enviárselo" a otra persona) es utilizando la llave privada que corresponde a esa dirección pública.

Mientras conserves la billetera, conservas las llaves privadas que te permiten disponer de los bitcoins que controla esa billetera. Por eso es aconsejable mantener *backups* del archivo wallet.dat.

¿Por qué nunca habrá más de 21 millones de bitcoins?

El límite de 21.000.000 que impone el protocolo es arbitrario; lo que importa es que, de acuerdo a las reglas que aceptan implícitamente todos los que utilizan el sistema, ese límite no puede ser superado, ni puede alterarse el ritmo en que se incrementa la masa monetaria. En este sentido, Bitcoin es absolutamente previsible – algo fundamental para un sistema monetario.

¿Cuándo dejarán de producirse los bitcoins?

Los bitcoins son generados como una recompensa al trabajo de los mineros, y dicha recompensa disminuye a la mitad cada 4 años. Hacia el año 2030 se habrán generado casi todos los bitcoins que llegarán a existir, aunque lo cierto es que seguirán generándose (cada vez menos) bitcoins. A la larga sólo ingresarán a la economía pequeñas fracciones de un bitcoin (cada vez menores) en el curso de varios años, pero la curva que representa el aumento de la masa monetaria continuará acercándose asintóticamente a 21.000.000.

¿Serán suficientes, en el futuro, 21 millones de bitcoins?

La escasez de bitcoins nunca va a ser un problema, porque cada bitcoin puede dividirse hasta el octavo decimal – y potencialmente aún más. Es decir que hoy puedes pagarle a alguien la cantidad de 0,00000001 bitcoin. Hablamos de una masa monetaria total integrada por – como mínimo – cuatrillones de unidades, así que bastaría un sólo bitcoin en circulación para abastecer de suficientes unidades monetarias a todo el planeta. En el futuro, de ser necesario, las unidades en uso podrían pasar a llamarse microbitcoins, nanobitcoins, etc.

¿Es Bitcoin un esquema piramidal?

Un esquema piramidal está basado en promesas incumplibles. Bitcoin NO es una compañía; no promete ni puede prometer: es un protocolo, una herramienta informática cuyo código puede ser libremente examinado por cualquiera, en cualquier momento.

¿Qué tiene de especial Bitcoin?

Es el único sistema que te permite transferir cualquier cantidad de riqueza de manera instantánea, a cualquier persona, desde y hacia cualquier lugar y en cualquier momento, sin tener que pagar tarifas abusivas, sin tener que preocuparte por el fraude o por el envilecimiento de la moneda, sin tener que pedir permiso a nadie y sin estar obligado a identificarte.

¿Cuál es el respaldo de Bitcoin?

El respaldo de Bitcoin son sus cualidades monetarias, ni más ni menos. ¿Cuál es, acaso, el respaldo del oro?… ¡sus cualidades monetarias! Quienes usan Bitcoin no tienen que confiar en las promesas de un gobierno, sino en las inmutables leyes de la matemática.

¿Tiene Bitcoin valor intrínseco?

Nada posee valor intrínseco; el valor es asignado a las cosas por los seres humanos. Puede decirse que las cualidades del oro son intrínsecas al oro, o que las cualidades de Bitcoin son intrínsecas a esta criptomoneda, pero el valor no se encuentra en el oro ni en Bitcoin: son los seres humanos los que valoran dichas cualidades.

Pero los bitcoins son intangibles: ¿no es esa una desventaja?

Es una ventaja. Gracias a esa cualidad (que los metales preciosos no tienen), los bitcoins pueden cruzar las fronteras instantáneamente, y es posible acceder a ellos desde cualquier lugar. Al mismo tiempo, Bitcoin permite esquivar las restricciones arbitrarias a la transferencia de valor (a diferencia del dinero digital que se mueve por los canales del sistema financiero tradicional).

Pero Bitcoin es deflacionario: ¿no es esa una desventaja?

A diferencia de lo que ocurre con el dinero de curso forzoso, es probable que el valor de tus bitcoins tienda a aumentar en relación a los productos que podrías comprar con ellos. Esta es una excelente noticia para la población productiva, y una pésima noticia para los que hoy controlan (o se benefician del control de) el sistema monetario. Al impedir la devaluación discrecional de la moneda, Bitcoin incentiva el ahorro y la inversión a largo plazo, a la vez que desincentiva el consumo irracional y el endeudamiento insostenible.

¿Es Bitcoin seguro?

Según los expertos, una transferencia entre direcciones Bitcoin es varias veces más segura que una transferencia entre cuentas bancarias (sin contar el riesgo que implica la forzosa intromisión de terceros en el sistema bancario). El código de Bitcoin está abierto al examen de todos los interesados, y su arquitectura criptográfica admite actualizaciones futuras para hacer frente a potenciales vectores de ataque (de ser necesario con décadas de anticipación).

¿Es cierto que Bitcoin ha sido hackeado?

No. El hackeo a las bases de datos de un sitio de intercambio de bitcoins NO es un hackeo a Bitcoin. Afirmar lo contrario equivale a decir que un hackeo a las bases de datos de un banco es un hackeo al dólar.

¿Cómo puede generar confianza un sistema monetario usado por sujetos anónimos?

El anonimato NO es algo que Bitcoin impone; es una elección que Bitcoin admite. Por otra parte, la confianza mutua no siempre es un requerimiento entre las partes involucradas en una transacción. Para prevenir el fraude, los usuarios de Bitcoin cuentan con diversos sistemas de reputación y servicios de depósitos en custodia (semejantes a los que ofrece eBay).

¿Es Bitcoin la moneda preferida de los criminales?

Bitcoin puede ser utilizado con fines ilícitos, así como el dólar, el rublo, el peso, etc. Cabe argumentar que Bitcoin es más eficiente que el dólar, el rublo, el peso, etc., y esto es absolutamente cierto, pero no hemos renunciado al avión – vehículo más eficiente que la bicicleta – ni al teléfono – medio de comunicación más eficiente que las señales de humo – porque pueden ser usados con fines ilícitos.

¿Puede Bitcoin ser prohibido?

Un gobierno podría intentar prohibir el uso de Bitcoin, pero controlar a los usuarios de Bitcoin es extremadamente difícil y extremadamente costoso. Para eliminar a Bitcoin hay que empezar nada menos que por eliminar Internet – aunque en el futuro Bitcoin podría funcionar incluso al margen de Internet.

Las prohibiciones no acabaron con BitTorrent, con Wikileaks, con las drogas ilegales, con la evasión impositiva, con la inmigración ilegal, con el trabajo "en negro", etc. etc… y tampoco acabarán con Bitcoin.

Con el aumento de la dificultad para obtener bitcoins por medio de la minería, ¿seguirá siendo rentable la minería "en casa"?

La minería casi nunca fue muy rentable para los que liquidan inmediatamente los bitcoins minados: al principio, por ejemplo, uno podía llegar a obtener cientos de bitcoins en un día de minería, pero no había manera de venderlos por más de USD 0,0001 (o ni eso). La minería sólo es rentable para los que entienden los fundamentos de Bitcoin, y por ende creen en el brillante futuro de esta tecnología. Así que todo depende del horizonte temporal del minero. Si has minado a principios de 2010 y todavía no has vendido los bitcoins obtenidos, has hecho un negocio formidable.

La dificultad para obtener Bitcoins por medio de la minería, ¿aumenta continuamente?

No. La probabilidad de adquirir bitcoins por medio de la minería depende de muchos factores, el principal de los cuales es el poder computacional que aporta el total de los mineros. La dificultad se ajusta automáticamente cada diez días para que el incremento de la masa monetaria ocurra según el ritmo programado. De modo que la dificultad puede disminuir, y lo ha hecho en reiteradas oportunidades (en general cuando el precio cae, lo cual desincentiva la minería en el margen).

Si el uso de Bitcoin creciera exponencialmente, ¿tendrían los mineros

cada vez más trabajo a cambio de cada vez menos bitcoins?

El sistema está diseñado para que la generación de bloques ocurra más o menos cada diez minutos, sin importar la cantidad de transacciones que cada bloque incluya. Más transacciones, de todas maneras, no significa necesariamente más trabajo para el minero (de hecho, podría incluso significar más bitcoins en concepto de *fees*). Y aunque en el futuro se van a generar menos bitcoins, hay que tener en cuenta que la misma restricción del incremento de la masa monetaria podría condicionar un aumento en el precio del bitcoin.

¿Acabará la minería en manos de un monopolio?

La gran diferencia entre la minería de bitcoins y la emisión de dinero de curso forzoso por un banco central es que la minería permanece abierta a cualquiera que desee involucrarse, es decir que no es posible monopolizarla. Nadie puede – ni podrá jamás – adueñarse de la minería de bitcoins. Es cierto que se trata de un mercado cada vez más competitivo, pero esa es una buena noticia – significa que la red estará a salvo.

Por otra parte, el incentivo para minar es directamente proporcional al precio del bitcoin, con lo cual un minero poco eficiente podrá beneficiarse aunque no logre obtener muchos bitcoins. Y nunca faltará quien pueda adquirir una ventaja competitiva simplemente accediendo a energía más barata.

¿Acabará siendo la minería el privilegio de unos pocos multimillonarios?

Los que invierten en granjas de minería de última generación no tienen garantías (recuerda, no es posible monopolizar la minería de bitcoins), y no les falta ni les faltará competencia. El modelo de los metales preciosos puede ayudar a entender este fenómeno: cualquiera puede involucrarse en minería de oro, por ejemplo, si cuenta con ciertos conocimientos y recursos. Algunos mineros serán más eficientes que otros; algunos tomarán mejores decisiones que otros; algunos tendrán mejor suerte que otros, etc. Empresas que hacen minería de metales preciosos hay miles; individuos o grupos de individuos aislados hay muchos más. Y esto es así aunque el negocio de la minería de

metales preciosos está distorsionado por la intervención estatal. En el caso de Bitcoin, las puertas están abiertas de par en par (y no pueden cerrarse): si quieres involucrarte en minería nadie va a pedirte una licencia.

¿Es sostenible la carrera tecnológica entre los mineros de bitcoins?

De hecho, la "carrera tecnológica" entre los mineros de bitcoins es la clave de la sostenibilidad de todo el sistema. Gracias a que la minería de bitcoins mejora con cada innovación en hardware y software, la red está segura.

¿Quién protegerá a la red cuando el sistema deje de premiar a los mineros con nuevos bitcoins?

Las tarifas de transacción irán cobrando más importancia cuanto más bajo sea el premio por bloque. En el futuro, los mineros se verán motivados a mantener los nodos generadores por la suma de pagos en concepto de tarifas que puedan acumular, más que por los bitcoins que sean capaces de generar.

Después de generado el último Bitcoin, ¿se acabará la minería de bitcoins?

No, puesto que lo que buscan los mineros no es, estrictamente, bitcoins, son un hash del siguiente bloque de transacciones. El que lo encuentra se queda con el premio en bitcoins (mientras haya premio) más el monto correspondiente a los *fees*.

¿Será Bitcoin destruido por la especulación monetaria?

En un mercado libre, todo lo que hacen los especuladores es comprar cuando pocos están comprando y vender cuando pocos están vendiendo. Lo quieran o no, así moderan las oscilaciones de los precios, y llevan liquidez a donde más se la necesita. Por otra parte, dado que el número de bitcoins es limitado, cualquiera que pretenda comprar cientos de miles de bitcoins generará tal aumento del precio (en gran medida por especulación de parte de los que ven subir el precio y postergan ventas de bitcoins) que probablemente

acabe sin efectivo antes de llegar a comprar 10.000. El dumping, en cambio, deprimirá el precio transitoriamente, ayudando así a expandir el mercado entre más participantes.

Las monedas tangibles de Bitcoin, ¿circularán a la par de otras monedas?

Los billetes y monedas tangibles de Bitcoin están pensados como artículos de colección, o bien para introducir en el mundo Bitcoin a gente que carece de mínimos conocimientos técnicos – no para basar en ellos el funcionamiento de la economía Bitcoin. Además, el fabricante de estos productos podría conservar las llaves privadas correspondientes a las unidades vendidas, con la intención de usarlas en el futuro (aunque asegure lo contrario). ¿Lo conoces?; ¿confías en él?; ¿confías en su entorno?…

La gran ventaja de Bitcoin es, justamente, que no depende de la capacidad o la buena voluntad del "emisor" de la moneda, sino de las inquebrantables leyes de la matemática.

¿Nos liberará Bitcoin de los bancos?

No necesariamente. Pero el problema del actual sistema monetario no reside en los bancos, sino en el dinero de curso forzoso impuesto por los estados – que hace posible, entre otras desgracias, el sistema de reserva fraccionaria con el banco central como garante de último recurso. Este sistema beneficia a los bancos a expensas de la población productiva, pero sólo puede funcionar a punta de pistola – y la pistola no la tienen los bancos, sino el Estado.

Los bancos funcionan como aliados del Estado (el actual marco regulatorio no les deja otra opción), pero no son los principales responsables del desastre que se avecina.

¿Mejorará Bitcoin la situación económica de los menos favorecidos?

La moneda no produce riqueza. La buena moneda es necesaria para que los recursos sean adecuadamente aprovechados, pero a la riqueza la producen los

individuos interactuando libre y voluntariamente. Dicho esto, es cierto que, en un mundo de monedas libres, las soluciones a los diferentes problemas sociales no se verían obstaculizadas tan a menudo por las arbitrariedades y las ineficiencias del sistema que hemos heredado.

¿Ayudará Bitcoin a que la riqueza se distribuya de manera más justa?

Si la recesión sigue profundizándose, los activos de los privilegiados por el actual sistema monetario y financiero pueden perder su valor muy rápidamente. Lamentablemente para ellos, el diseño de Bitcoin impide la concesión de privilegios.

¿Ayudará Bitcoin a prevenir las guerras?

Las guerras NO pueden financiarse si no es mediante la violencia y el fraude. ¿Cuánta gente apoyaría una declaración de guerra a un país distante si tuviera que pagar su parte de la aventura directamente de su bolsillo? La realidad es que los gobiernos nos obligan a financiar sus guerras básicamente mediante endeudamiento e inflación, y esto sólo es posible gracias al control del sistema monetario y financiero. Por lo tanto, los pacifistas deberían ser los primeros en abrazar a Bitcoin.

¿Necesitamos más bitcoins en circulación para activar la economía?

La moneda es una institución social que surgió espontáneamente como mecanismo para facilitar los intercambios, preservar el valor económico y proporcionar una unidad de cuenta (una medida de valor común). La moneda libre (no monopolizada por los estados) puede ayudar a asignar los recursos en función de su productividad, y así FACILITAR la creación de riqueza, pero una de las cualidades más importantes de la buena moneda es su escasez relativa. Más dinero en circulación – no importa cómo se distribuya – no va a solucionar el problema del estancamiento económico y la pobreza. De hecho, el uso de la fuerza para distribuir la riqueza por medio del control del sistema monetario y financiero es la principal causa de la recesión y las consiguientes penurias económicas.

SEXTA PARTE

TUTORIALES

1 • Cómo obtener una billetera

La billetera (o cartera) Bitcoin es en realidad un archivo que necesitamos para enviar y recibir bitcoins; puede decirse que este archivo "contiene" nuestros bitcoins, aunque en realidad lo que contiene son llaves criptográficas (claves privadas, únicas, irrepetibles y secretas) que nos hacen dueños de nuestros bitcoins y nos permiten autorizar pagos (transferir la posesión de nuestros bitcoins).

Obtener una o varias billeteras Bitcoin es fácil; a continuación describiremos las dos maneras más conocidas de hacerlo:

Por medio del cliente Bitcoin

El cliente oficial de Bitcoin es un programa que se puede instalar en cualquier computadora con sistema operativo Windows, Mac o Linux, descargándolo desde bitcoin.org. Automáticamente creará una billetera y comenzará a descargar el historial de transacciones (cadena de bloques). Este último paso puede demorar más de una hora. Es necesario estar online sólo para enviar bitcoins desde la propia billetera; no para recibir bitcoins.

Por medio de servicios online (ej.: Flexcoin)

Existen sitios que ofrecen servicio de billetera *online*. No requieren la instalación de ningún programa; tan sólo hay que registrar un nombre de usuario y una contraseña por cada cuenta que uno desee abrir. Debe tenerse presente que las llaves privadas que controlan los bitcoins acreditados en dichas cuentas no quedan almacenadas en nuestra computadora (o *pendrive*, o CD, o tarjeta), de modo que la seguridad no queda completamente en nuestras manos. Si se guardan muchos bitcoins en este tipo de cuentas, es recomendable utilizar una contraseña extensa (al menos 12 caracteres), exclusiva y difícil de descifrar, y asegurarse de no perderla/olvidarla.

Lo más reciente

Hay una nueva generación de servicios de billeteras online que no están expuestas a violaciones de la seguridad (debido a que las llaves privadas son encriptadas en el navegador del usuario). El ejemplo más prominente de esta clase de servicio es MyWallet, de blockchain.info.

LINK A LISTA DE SITIOS QUE OFRECEN BILLETERAS ONLINE:

https://en.bitcoin.it/wiki/category:ewallets

Todas las opciones mencionadas proveen una o varias direcciones Bitcoin que aparecerán en pantalla, las cuales pueden utilizarse para recibir bitcoins en la propia billetera. Una dirección Bitcoin es algo similar a esto:

1Q4KHiT35UQE2KvZZMbuTBbagjqDgfqj78

2 • Cómo obtener bitcoins

Luego de obtener una billetera (o cartera) Bitcoin, hay varias maneras de obtener bitcoins:

1 - Bitcoin Faucet (grifo o canilla de bitcoins):

Este servicio fue creado por Gavin Andresen, el programador que actualmente lidera el proyecto Bitcoin, con el fin de promover su adopción masiva. Solía entregar 5 bitcoins a cualquiera que los solicitara, pero actualmente sólo pueden obtenerse 0,001 bitcoins. Recomendable sólo para debutantes ansiosos por utilizar la moneda del futuro. Otros sitios similares a Bitcoin Faucet son *Daily Bitcoins*, *CoinAd* y *BitVisitor*; a diferencia de aquél, estos permiten obtener fracciones de bitcoin todos los días (en el caso de *BitVisitor*, cada 5 minutos).

2 - Sitios de compra/venta de bitcoins:

El más utilizado es MtGox. Pero hay muchos otros sitios que facilitan el intercambio de todo tipo de divisas por bitcoins y admiten diversos sistemas para transferir los fondos. *Bitinstant* y *BitcoinNordic* venden bitcoins a través de cientos de miles de puntos de venta distribuidos en todo el mundo.

3 - Sitios de compra y venta online:

Ej: Conbitcoin (en español), Bitmit (símil eBay) o CoinDL (símil iTunes).

4 - Sitios que aceptan pagos por medio de Western Union o Liberty Reserve:

Ej.: Nanaimo Gold.

5 - Sitios que aceptan oro o plata a cambio de bitcoins:

Ej.: Coinabul.

6 - Sitios que aceptan Linden Dollars (la moneda digital utilizada en Second Life) a cambio de bitcoins:

Ej.: VirWoX.

7 - Sitios que aceptan pagos mediante PayPal o transferencia bancaria:

Ej.: FastCash4Bitcoins.

8- Aceptar bitcoins como pago por bienes o servicios.

Es posible fijar un precio en cualquier moneda y optar por ajustar automáticamente los precios nominados en bitcoins, para que el costo de los productos no se vea afectado por las fluctuaciones en el tipo de cambio. Por medio de Bit-Pay, los pagos en bitcoins además pueden ser automáticamente convertidos a la moneda que el comerciante prefiera.

9- Encontrar personas dispuestas a vender bitcoins:

Se pueden localizar por medio de tradebitcoin, LocalBitcoins o foros especializados, entre otros sitios. En general se trata de "antiguos" mineros que disponen de grandes cantidades de bitcoins, aunque también hay operadores que compran bitcoins y los venden cobrando una comisión. Conviene elegir un lugar neutral para realizar la transacción (como un bar o restaurante con wi fi).

10- Involucrarse en "minería" de bitcoins:

Debido a los incrementos en la dificultad para obtener bitcoins de esta manera – relacionados con el creciente poder computacional que aporta el total de los mineros – hoy en día es necesario contar con potentes tarjetas de video, además de participar en un pool minero, para "extraer" una cantidad apreciable de bitcoins. Hace mucho tiempo que la minería dejó de estar al alcance del usuario común de una PC.

11- Mercados que funcionan sin intermediarios:

Con el fin de minimizar el riesgo de fraude, estos sitios proveen acceso a la reputación y al historial de transacciones de todos sus miembros. Ej: *bitcoin-otc* (sin duda, no apto para novatos) o Bitcoinary (interfaz más amigable, aunque lleva menos tiempo online).

12 - Juegos basados en Bitcoin:

Obsequian fracciones de Bitcoin para que el que quiera pueda jugar. Ej: Strike Sapphire (casi no), Seals with Clubs (póker) y Dragon's Tale (MMORPG).

13- Otros:

FeedZeBirds (retweetea por bitcoins); CoinWorker (usa tu mente y cobra en bitcoins); Forbitcoin (¿qué harías a cambio de bitcoins?); Rugatu (donde las mejores respuestas se premian con bitcoins).

3 • Cómo crear una “caja fuerte” de bitcoins en sólo 4 pasos

Siguiendo estas sencillas instrucciones, podrás acceder en cuestión de minutos a un nivel de seguridad que ni el mejor banco suizo puede ofrecerte. Además, tus ahorros estarán disponibles para ser utilizados en cualquier momento, dondequiera que estés.

I) Descarga la última versión del cliente Bitcoin en una computadora razonablemente segura (con firewall, antivirus y parches actualizados, y no utilizada para navegar sitios inseguros). No es necesario que esperes a que se complete la sincronización con la red para pasar al siguiente paso.

II) Copia y pega una o más direcciones Bitcoin públicas (las que se ven al clickear el botón “Recibe monedas”) **en un email, y envíatelo a ti mismo.** Estas direcciones públicas son las que utilizarás más adelante para recibir bitcoins.

III) Clickea la opción “Encriptar cartera” (en la pestaña **“**Configuración**”**), y usa una contraseña de al menos 13 caracteres, preferentemente con mayúsculas, minúsculas, números y otros signos, y que no incluya palabras. Anota la contraseña en papel y guárdala en más de un lugar, por si te la olvidas.

IV) Clickea la opción “Backup de cartera” (en la pestaña “Archivo”), y elige el destino del archivo-cartera, es decir del archivo que te permitirá, el día de mañana, gastar los bitcoins ahorrados. Es conveniente hacer copias de este archivo (denominado wallet.dat) en más de un pendrive, y enviarlo como archivo adjunto a más de una cuenta de webmail (ej: yahoo + gmail).

>> Puedes llevar un control de los bitcoins recibidos en cada dirección – sin tener que recurrir al archivo-cartera ni al software de Bitcoin – utilizando el blockexplorer.

>> Algo importante: si decides gastar bitcoins que están guardados en tu archivo-cartera, después de hacerlo tienes que hacer un nuevo backup (cuidado: el anterior backup ya no sirve). Las nuevas versiones del cliente van a ofrecer soluciones automáticas para este problema.

4 • Introducción a la minería

¿Qué es la Minería de bitcoins (Bitcoin Mining)?

Generar bitcoins es conocido como “minar”, un término que remite a la minería de metales preciosos. La minería de bitcoins es el proceso por el cual se generan los “bloques” de una “cadena” (ver “Qué es Bitcoin“, en la PRIMERA PARTE), cuyo propósito es el de verificar la legitimidad de las últimas transacciones (transferencias de bitcoins) que se han llevado a cabo. El agregar un nuevo bloque a la cadena es un proceso difícil que requiere un gran poder de cómputo.

¿Cuál es el incentivo para producir un bloque?

Ésta es la parte interesante: aquel que sea el primero en “producir” (encontrar) un nuevo bloque, recibirá Bitcoins a modo de recompensa por su trabajo. Desde el punto de vista de la red, los mineros proveen seguridad al sistema, verificando las transacciones que se llevaron a cabo e impidiendo que haya errores de cómputo y crédito. Todo esto es realizado automáticamente por el software de minería.

¿Qué herramientas necesito para minar bitcoins?

En un principio sólo se precisaba una computadora común y el mismo programa utilizado para manejar la billetera: el Cliente Bitcoin. Hoy en día, el proceso se tornó un poco más complicado y especializado, pero aún está al alcance de cualquiera con acceso a un ordenador con una buena tarjeta gráfica.

¿Cuántos bitcoins obtengo cada vez que encuentro un bloque?

En la actualidad, la recompensa por encontrar un bloque es de 25 BTC (veinticinco bitcoins). Esta cantidad se reducirá a la mitad a fines de 2016 y seguirá reduciéndose un 50% cada 4 años aproximadamente.

¿Cada cuánto tiempo se descubre un bloque?

La red Bitcoin crea y distribuye un lote de nuevos bitcoins (25 en la actualidad) aproximadamente cada 10 minutos, de manera aleatoria, a alguien que esté ejecutando el software. La probabilidad de recibir un lote depende del poder computacional aportado, en relación a la suma del poder computacional

que aportan todos los demás mineros.

¿Cómo se mide el poder de cómputo de un minero?

El poder de cómputo de un minero se mide en **MHash/s** (Mega Hashes por segundo), y a la capacidad para producir estos Mega Hashes se la denomina **Hash Rate** (Poder de Hasheo).

¿En qué consiste la dificultad para descubrir un bloque?

Es simple: si yo fuera el único minando, mi probabilidad de encontrar el próximo bloque sería del 100%. Pero si hubieran 10 mineros (todos con igual poder de hasheo) la probabilidad de encontrar el próximo bloque, para cada uno de ellos, sería del 10% – es decir que la dificultad sería más elevada.

¿Cada cuánto tiempo cambia la dificultad?

El sistema está diseñado para que la dificultad cambie cada 2016 bloques, es decir cada 2 semanas. El propósito de este ajuste automáticamente controlado es que el ritmo de producción se mantenga fiel a las reglas que fija el protocolo de Bitcoin.

¿Cuál es la dificultad actual?

La dificultad puede subir o bajar, dependiendo de las circunstancias del mercado. Hacer un análisis de la dificultad es importante para saber si es más conveniente comprar o minar bitcoins en un momento dado.

Dificultad actual

Próxima Dificultad Estimada

¿Qué son los Pools de Minería?

Debido a la alta dificultad, hoy en día es necesario un gran poder de hasheo para tener una chance razonable de encontrar un bloque (y hacerse con los 25 BTC correspondientes). Es por ello que los mineros comenzaron a agruparse y a combinar su poder de cómputo para aumentar la probabilidad de ser beneficiados. Cada vez que un grupo de mineros encuentra un bloque, la recompensa (los 25 BTC) se reparte entre sus miembros de manera proporcional al poder de hasheo aportado por cada uno de ellos. A estos

grupos de minería se los denomina **Pools**. Actualmente, casi todos los mineros trabajan afiliados a Pools de minería.

¿Qué es un "Rig"?

Los **Mining Rigs** (inglés para plataformas o equipos de minería) son ordenadores usados para minar bitcoins. Un **rig** puede ser una computadora armada y operada con ese único propósito – dedicada exclusivamente a la minería – o bien puede ser un ordenador utilizado con otros fines (trabajo, juegos o ambos), destinado a la minería sólo parte del tiempo.

¿Qué es la Minería con GPU?

La minería con GPU (*Graphics Processing Unit* = Unidad de Procesamiento Gráfico), es el proceso por el cual se utiliza una tarjeta gráfica (o placa de video) como fuente de cómputo para producir bitcoins. La minería con GPU ha sido, entre el 2011 y el 2012, la principal forma de generar bitcoins debido al gran poder de Operaciones de Punto Flotante por Segundo (FLOPS) que poseen estas tarjetas gráficas. Pero actualmente las GPUs están siendo rápidamente desplazadas por nuevas tecnologías – mucho más eficientes – aplicadas a la minería Bitcoin (FPGA, ASIC).

¿Qué es la Minería con CPU?

La minería con CPU (*Central Processing Unit* = Unidad Central de Procesamiento, comúnmente llamado microprocesador), es el proceso por el cual se utiliza el microprocesador de un ordenador para hacer el trabajo de cómputo necesario para conseguir Bitcoins. Esta era la forma más común de minar en el pasado, pero cayó en desuso al incrementarse la dificultad para minar bitcoins (una GPU tiene un poder de cómputo unas 800 veces mayor que el de una CPU).

ADDENDUM

POR QUÉ LA MONEDA DEL FUTURO NO SURGIRÁ DE LAS REDES SOCIALES

I

Sabemos que las nuevas tecnologías pueden desencadenar transformaciones notables en un sistema económico. Pero una nueva tecnología no será capaz de inducir un **cambio radical** si no incrementa de alguna manera la productividad (o levanta las barreras a la productividad) de todas las formas que adopta el capital en tal sistema.

Un gran salto evolutivo requiere algo más que una gran mutación; la mutación tiene que ser además oportuna, y afectar a un instrumento que pueda, a su vez, afectar a todos los demás instrumentos. ¿Se entiende a lo que apuntamos?

El rol de la moneda es lo suficientemente general como para cambiarlo todo. Nuestros amos lo han sabido siempre; por eso nos han enseñado que el monopolio sobre la moneda es algo natural; por eso han entorpecido la verdadera innovación en la materia…

Las monedas reglamentarias continúan hoy atadas a los estados, de modo que los jefes de cada tribu siguen teniendo el poder de erosionar su valor, de obligarnos a utilizarlas, de resolver cómo y para qué debemos utilizarlas, etc. De ello deriva una situación curiosa: mientras las nuevas tecnologías proliferan a nuestro alrededor, vivimos en un estado de incertidumbre económica digno de la edad de piedra.

Hasta la creación de Bitcoin, las nuevas tecnologías prácticamente no habían alcanzado a la moneda, salvo para transformarla en una herramienta más de control.

II

Bitcoin marca el comienzo de una nueva era en la historia de la moneda: la era de la evolución consciente – todo lo anterior quedará en la prehistoria, como el envío de cartas o documentación por correo común; la difusión de música por medio de discos; la lectura de las noticias en periódicos de

papel… todas estas prácticas van siendo arrojadas a la prehistoria sin mayores trámites.

Es un proceso inexorable: todo lo que pueda reducirse a bits de información será transformado, replanteado, corregido, adaptado, perfeccionado… a una velocidad inimaginable para las generaciones que nos precedieron. Sin embargo, quienes integran las nuevas generaciones no se sienten privilegiados – Internet es parte de su realidad cotidiana. Preguntarles para qué sirve Internet es casi como preguntarles para qué sirven los cinco sentidos.

De modo que no hay vuelta atrás. Internet mediante, la mejor moneda posible deja de ser un hallazgo fortuito, y pasa a ser una creación infinitamente perfectible; pasa a ser, en realidad, **la mejor moneda concebible.**

Una moneda que es fruto del libre mercado siempre será superior a una moneda sometida al monopolio estatal, por la misma razón que un almuerzo en un restaurante siempre será mejor que una ración de comida asignada por un gobierno comunista. Pero una moneda que, además, funciona en base a un software de código abierto, y que dado su carácter descentralizado es resistente a la intervención estatal, no sólo es superior al dinero de curso forzoso; hasta puede decirse que es otra cosa.

III

Sin dinero de curso forzoso, los estados no podrían endeudarse infinitamente a expensas de las futuras generaciones, ni robar el fruto de nuestro esfuerzo por medio de inflación y otros impuestos, ni sacrificarnos en guerras inútiles. En efecto, el dinero impuesto por la fuerza mantiene vivo al aparato estatal a expensas de la población productiva. Bitcoin – la pesadilla de todo banco central – actúa justo en sentido contrario: restableciendo la autonomía individual – ya que no puede ser utilizado como herramienta de control, fraude y usurpación por parte del Estado.

Pero lo que distingue fundamentalmente a Bitcoin del dinero emitido por los estados no es la tecnología criptográfica que lo respalda, ni las reglas que establece su protocolo, ni la comunidad en la cual se originó el proyecto; lo peculiar de Bitcoin – ¡horror de horrores! – es que su adopción es completamente libre y voluntaria, así como la elección de los fines a los que

puede ser destinado. Quienes eligen Bitcoin no lo hacen bajo amenaza; por el contrario, tienen muy buenas razones para hacerlo.

De acuerdo a la imperecedera definición de Aristóteles, la buena moneda facilita el intercambio indirecto y la preservación del valor, y sirve como unidad de cuenta. Dichas funciones obedecen a los siguientes atributos de un determinado bien: durabilidad, portabilidad, fácil almacenamiento, difícil falsificación, homogeneidad, divisibilidad, fungibilidad, amplia distribución geográfica y, sobre todo, baja proporción entre su producción anual y el stock de existencias.

Por lo tanto, Bitcoin abriga el potencial de convertirse en la moneda por excelencia, y como tal, de actuar a un nivel mucho más profundo – y difundirse más rápidamente – que las redes sociales basadas en afinidades o en contactos laborales. ¿Por qué?

IV

Toda red social de cierta envergadura da origen a nuevas combinaciones de factores productivos, e impulsa el descubrimiento de nuevas formas de capital. Indudablemente, Facebook aporta eficiencia al conjunto de la economía, y lo hace de un modo explícito y directo. Pero la clave de su éxito – una plataforma que facilita el contacto entre personas con intereses comunes o complementarios – es también la razón por la cual no ha llegado a producir cambios económicos de fondo.

Los beneficios de una moneda digital, libre y descentralizada no se limitan a individuos conscientemente vinculados entre sí. El verdadero potencial de Internet ni siquiera puede ser imaginado en ausencia de una moneda digital, libre y descentralizada. Y no, no basta con que sea digital: como el e-mail, la moneda digital es inútil – y hasta contraproducente – si no admite el intercambio libre y descentralizado. ¿Qué sería del e-mail si para enviar un mensaje tuviéramos que llenar un formulario, conseguir la autorización de un funcionario estatal y pagar el costo de envío precisamente a quienes lo están obstaculizando?

V

La moneda es una de esas maravillas cotidianas que damos por descontadas. Pero aún en sus formas primitivas, cada innovación monetaria representó en su día un salto evolutivo descomunal. Esto se debe a que la moneda potencia uno de los rasgos más peculiares de la interacción humana: el intercambio para la mutua satisfacción de necesidades.

Con la irrupción de la moneda se multiplican las oportunidades para el intercambio pacífico entre seres humanos, y por ende las posibilidades de hallar valor en lo diferente. El temor a lo foráneo cede ante las oportunidades que – ahora sí – pueden vislumbrarse. Así es como la institución moneda nos eleva económicamente (por encima del nivel de subsistencia) y moralmente (por encima de los mandatos tribales).

La moneda nos une de un modo a la vez profundo y abstracto, en una red de interacciones tan infinitamente compleja y cambiante que no es posible representarla sin hacerle injusticia. La moneda nos conecta – aún si no lo sabemos, aún si no lo queremos – con millones de personas que no conocemos y que muy probablemente nunca llegaremos a conocer; millones de personas que, sin compartir nuestros gustos, opiniones o creencias, interactúan con nosotros en forma espontáneamente coordinada y mutuamente beneficiosa.

Cuando gastamos nuestro dinero en un lápiz, o en un par de zapatos, estamos enviando señales a millones de personas en todo el mundo; de alguna manera les estamos diciendo: “me sirve su trabajo”; “me alegra que se dedique a esto”; “no abandone tal proyecto”; “invierta más en aquello”, etc. Gracias a la moneda, no hace falta conocerlos para expresarles nuestro reconocimiento, gratitud y aprecio.

VI

Podemos usar la moneda – como usamos el lenguaje – sin conocer sus reglas, precondiciones, orígenes, etc. Pero comprender la manera en que la moneda funciona requiere cierto entrenamiento: es necesario ampliar el foco, situarse por encima de las relaciones personales – una predisposición que, según parece, no está grabada en nuestros genes.

Los vínculos que propician las redes sociales son experimentados y valorados en forma directa por sus integrantes, quienes permanecen conectados por motivos explícitos, ejerciendo un alto grado de control sobre las señales que emiten y reciben. En cambio, por medio de la moneda nos llegan señales útiles pero enigmáticas, y emitimos señales cuyo rastro se pierde casi de inmediato. Ante estos fenómenos, nuestro sentido común se rebela: "Si tenemos poco y nada en común con la inmensa mayoría de los que participan en tal sistema… ¿cómo se dirige el proceso productivo?; si ni siquiera nos conocemos… ¿cómo es posible que nos organicemos efectivamente para crear, producir y distribuir tantos bienes y servicios?".

Al igual que la institución lenguaje, la institución moneda no surgió por decreto, y ciertamente no requiere una dirección central para funcionar. De hecho, establecer una dirección central es la mejor forma de entorpecer su funcionamiento; esto es, de obstaculizar el acceso a la prosperidad – cuando no a la mera supervivencia – de millones de personas que sólo pueden coordinar sus acciones de manera eficiente gracias al mecanismo de precios.

VII

Cualquier interferencia coactiva en el mecanismo de precios – naturalmente abierto y descentralizado – corrompe el delicado sistema de incentivos que estructura una economía compleja, y supone un deterioro general en el nivel de vida. En otras palabras, no hay mejor mecanismo que el de los precios para optimizar la satisfacción de nuestras necesidades.

Un precio es una invitación a considerar las mejores maneras de hacer uso de los recursos disponibles; cuando es representativo del valor económico de un determinado producto, nos permite procesar una cantidad inimaginable de información. De hecho, un precio será tanto más fiable cuantas más interacciones libres sea capaz de reflejar.

Pero los precios carecen de significado sin una referencia sólida y ampliamente aceptada, externa a cada transacción; sin una herramienta que permita establecer unidades de valor, para que los agentes económicos puedan informarse, comparar y hacer cálculos antes de tomar decisiones. Estamos hablando, por supuesto, de la moneda.

VIII

La buena moneda es la clase de instrumento que resulta tanto más útil cuantas más personas deciden adoptarlo. Esto no significa que su utilidad puede aumentarse forzando a la gente a adoptarla: por el contrario, sólo puede probarse que una moneda es superior a otra si la gente es libre de elegirla. Al fin y al cabo, los fines que guían la elección de una moneda son los mismos para todos los seres humanos: intercambio indirecto y preservación del valor.

Cabe esperar entonces que – en ausencia de coacción – prevalezca la mejor moneda disponible. Sólo en un grupo humano muy pequeño y extremadamente aislado es posible desconocer o desalentar el uso de un medio de intercambio reconocido fuera de ese grupo. Pero una comunidad que prescinde del conocimiento y las acciones de innumerables individuos ajenos a ella (esto es, de la división del trabajo en un mercado extenso) cae indefectiblemente en el nivel de subsistencia.

Aún aquellos productos que son valorados exclusivamente dentro de una determinada comunidad, en general sólo pueden obtenerse recurriendo a otros productos e insumos, y por ende a precios que no se han formado en el seno de tal comunidad. Es por eso que las redes sociales en Internet, señaladas por su apertura y constante metamorfosis, requieren – más que ningún otro tipo de comunidad – una referencia monetaria externa.

IX

En toda red social interesa la identidad de cada uno de los miembros (sea ésta real o creada para interactuar con los demás en ese contexto). Una red social puede apoyarse en la calidad de las relaciones personales entre sus miembros, o en el aprecio que ellos se tienen, o en la confianza mutua, o en alguna simpatía o afición compartida, o – al menos – en algún interés común o complementario. Pero este tipo de relaciones, aunque vitales para facilitar la asignación del crédito, no sostienen a una economía compleja.

Moneda y crédito son instituciones complementarias pero fundamentalmente diferentes. La institución moneda funciona en base a reglas abstractas; la institución crédito involucra relaciones y acuerdos personales. En el otorgamiento de un crédito entran en juego – de manera más o menos formal,

según el caso – la reputación y capacidad de persuasión de quien lo pide, el discernimiento de quien lo otorga y la confianza entre las partes. Ambos, acreditante y acreditado, apuestan a lo mismo con diferentes recursos. ¿Qué mejor punto de encuentro para ellos que las comunidades digitales?

Pero sin el respaldo de una moneda de valor ampliamente reconocido, no es posible hacer pesar la reputación más allá del círculo que la estima y que puede dar fe de la misma. En otras palabras, es la moneda la que sirve para medir el valor relativo de la reputación personal, y no viceversa – como proponen los partidarios de las "monedas locales" y de las formas sofisticadas del trueque.

Los instrumentos más innovadores para asignar el crédito seguirán surgiendo, indudablemente, de las comunidades digitales. Lo que no puede ser definido en las relaciones que forjan estas comunidades (al menos no con precisión) es el valor económico de los créditos otorgados. Para ello seguirá siendo necesario contar con una herramienta que permita capitalizar el crédito fuera de la comunidad.

Las leyes de la economía, como las de la física, no son modificadas por los avances tecnológicos.

X

El valor aportado por alguien dentro de una comunidad (no aislada) no puede ser correctamente calculado ni aprovechado si no se traduce a unidades de valor aceptadas fuera de esa comunidad. ¿De qué le sirve a un gran pianista el reconocimiento de su público – si este reconocimiento no es monetario – cuando necesita los servicios de un plomero? Probablemente no consiga un buen plomero en ninguna de las comunidades (digitales o no digitales) en las que participa, ni pueda eventualmente pagarle con entradas para su próximo concierto (por más valiosas que éstas sean para otras personas).

La moneda es, en sí misma, una mercancía, utilizada para facilitar el intercambio de otras mercancías. Cuando a una población se la priva de una buena moneda, toda clase de inconsistencias, distorsiones y fricciones vienen a entorpecer el funcionamiento del mercado. Cabe entonces preguntarse: ¿a quién beneficia la circulación de mala moneda?… En el largo plazo, a nadie; forzar

la circulación de mala moneda – una cuestión de supervivencia para casi todos los gobiernos en el mediano plazo – es algo semejante a contaminar la red de agua potable: todos padecerán las consecuencias.

Ahora bien, aún teniendo que soportar el peso de sistemas legales extremadamente represivos – que imponen el curso de tal o cual dinero bajo la amenaza de duras penas – la gente gravita siempre, tarde o temprano, hacia la mejor moneda disponible, buscando la protección o la sólida referencia que ésta proporciona. La buena moneda emerge de la clandestinidad una y otra vez, en la última etapa de cada ciclo económico, para restituir el tejido social que la violencia gubernamental ha destrozado: no otro ha sido el rol del oro durante los últimos cinco mil años.

El valor del oro no depende del efímero poder de un Estado, ni del compromiso de un grupo de individuos conscientemente vinculados entre sí; por eso mismo se ha reconocido y se sigue reconociendo prácticamente en todas partes. Si preferimos que nos paguen con monedas de oro antes que, digamos, con bonos de un club de trueque barrial, no es debido a una mera inclinación personal: el oro es, objetivamente, mejor moneda.

Y la buena moneda no sólo permite satisfacer toda clase de necesidades de manera eficiente (con la menor demora y pérdida de valor posibles); también hace viables aquellos proyectos capital intensivos que una comunidad suele necesitar, pero que no pueden ser financiados – y mucho menos llevados a cabo – sólo por individuos conscientemente vinculados entre sí.

XI

La eficiencia que provee la división del trabajo sólo es posible gracias a la institución moneda. Esta conecta a los individuos y a las comunidades complementando sus atributos, potenciando sus capacidades y proyectando sus logros. Es por eso que la manipulación política de la moneda está condenada a fracasar una y otra vez: la institución moneda simplemente no nació como una herramienta de control social – la violencia la torna inefectiva; las fronteras la fosilizan.

El valor que representa una unidad de una moneda libre (no impuesta por la fuerza) no se decide en cada grupo humano por separado, así como la distancia

que representa un metro no se decide en cada familia, club o red social. Estas son magnitudes que derivan su utilidad de la adopción voluntaria y descentralizada.

¿Y por qué millones de personas van a elegir un signo monetario, entre muchos otros, para medir el valor económico? Por las mismas razones que eligen usar el metro – en lugar de su antebrazo – para medir longitudes con precisión, o enviar e-mails – en lugar de cartas certificadas – para comunicarse a la distancia: eficacia y eficiencia.

Para que la moneda de referencia pueda cumplir con sus funciones en un mercado extenso, los fundamentos que dan valor a cada unidad monetaria tienen que ser tan ciertos, tan confiables y tan incorruptibles como la distancia que representa un metro.

En pocas palabras…

La mejor moneda disponible no es la que sirve en el seno de tal o cual grupo humano, sino la que – objetivamente – mejor cumple con las funciones monetarias (facilitar el intercambio indirecto y la preservación del valor, y servir como unidad de cuenta).

La mejor moneda disponible es el commodity que más fácilmente – y con menor pérdida de valor – puede ser intercambiado, en todo momento, por cualquier activo.

La irrupción de una moneda infinitamente superior a la mejor moneda disponible incrementa la productividad de todas las formas que adopta el capital. Por lo tanto, esta nueva moneda tiene el potencial de transformar completamente a un sistema económico.

Bitcoin es mucho más que la mejor moneda disponible; dada su naturaleza, Bitcoin aspira a ser la mejor moneda concebible. Y como tal, puede llegar a desencadenar una explosión de fuerzas productivas que desafían a la imaginación más fecunda.

Bitcoin será el salto evolutivo que hará posibles todos los próximos saltos evolutivos.

EPÍLOGO

LO QUE NOS MOTIVA

A esta altura, el colapso del sistema financiero tal como lo conocemos es algo tan inevitable como la resaca después de una borrachera. No hace falta un postgrado en economía para entender que nadie puede vivir indefinidamente por encima de sus ingresos. Esto, que es válido para cualquier individuo, también lo es para familias, clubes, ciudades y países.

Lamentablemente, muy pocos están tomando las medidas necesarias para protegerse de la gran depresión que se avecina. Los adoctrinados, los apáticos y los interesados en mantener el **statu quo** integran la inmensa mayoría de la población. Los demás están demasiado ocupados intentando sobrevivir a la expansión del aparato estatal. ¿Qué hacer, entonces, al respecto?

Nuestra posición es semejante a la de un científico que pretende evacuar a una población de la zona en la que impactará un asteroide. Él ha determinado en qué momento y en qué sitio caerá el enorme cuerpo rocoso, pero los líderes de la aldea que está a punto de ser borrada del mapa le explican amablemente que no hay nada que temer, "puesto que los cuerpos celestes no son más que antorchas utilizadas por los dioses para orientarse en la oscuridad."

El tiempo se acaba; el asteroide se acerca… ¿discutimos con los que sostienen teorías erróneas… o salvamos a los que aún pueden ser salvados?; ¿desafiamos el **statu quo**… o nos dedicamos a ayudar a quienes han decidido escapar a tiempo?; ¿nos preocupamos por lo que dice de nosotros una mayoría ignorante… o por lo que dirán de nosotros las futuras generaciones?

Enfrentémoslo: el conocimiento implica una responsabilidad que no es posible eludir (no hacer nada también tendrá consecuencias). Así lo

entendió Erik Voorhees , y por eso decidió abandonar sus otros trabajos para dedicarse por completo a emprendimientos relacionados con Bitcoin (Bitinstant, SatoshiDice, FeedZeBirds). He aquí su justificación:

“Esta nueva tecnología tiene el potencial – más que todas las obras filantrópicas existentes – de corregir la esencia misma de los problemas más graves que enfrenta la humanidad.”

GLOSARIO

HASH: es una función que transforma cualquier número o serie de caracteres (entrada) en un resultado de tamaño fijo (valor hash), pero no permite revertir el proceso fácilmente. Para hacerlo – para determinar la entrada a partir del valor hash – es necesario probar con todas las posibles entradas. Para un ejemplo de una función hash podemos considerar una raíz cuadrada: la raíz cuadrada de 17202 es fácil de calcular (alrededor de 131.15639519291463). Una simple función hash, entonces, puede ser los últimos 7 dígitos del resultado así obtenido (en este caso, 9291463). Contando sólo con ese dato es muy difícil averiguar el número inicial del que este provino y, básicamente, uno debería pasar por todas las posibilidades para determinarlo. Pero quien conozca la cifra inicial podrá reproducir el valor hash muy fácilmente. Los hashes criptográficos modernos, como el SHA-256, son una versión mucho más segura y compleja de esto.

ALGORITMO DE ENCRIPTACIÓN (o cifrado) TRADICIONAL: es una función que transforma un mensaje en una serie ilegible aparentemente aleatoria, usando una clave de encriptación que permite acceder al mensaje original sólo a quienes la conocen. Por medio de la encriptación, la información privada puede ser enviada públicamente por internet sin mayor riesgo de que otros puedan tener acceso a ella.

CRIPTOGRAFÍA DE CLAVE PÚBLICA : es un método de cifrado en el que toda clave privada tiene una clave pública correspondiente, a partir de la cual es imposible determinar la clave privada. Nos permite publicar una clave que cualquiera puede usar para enviarnos un mensaje cifrado sin que tengamos que compartir nuestra clave privada.

FIRMA DIGITAL : es la información que puede adjuntarse a un mensaje para indicar que el remitente del mismo es el dueño de una clave privada correspondiente a una determinada clave pública, sin necesidad de exponer la primera. Fuera de la red de Bitcoin, las firmas digitales son generalmente usadas para autenticar la identidad del remitente de un mensaje.

CLIENTE BITCOIN: es un programa que se usa para recibir y enviar bitcoins. El más popular es el cliente estándar de Bitcoin, aunque existen muchas otras versiones con diferentes características.

CARTERA, **BILLETERA** O ***WALLET***: puede ser sinónimo del cliente Bitcoin (o de una cuenta en un servicio de cartera online), o bien del archivo *wallet.dat*, empleado por el cliente estándar para alojar las claves privadas que nos permiten controlar nuestros bitcoins.

DIRECCIÓN BITCOIN PÚBLICA: es una serie de caracteres, como "1Q4KHiT35UQE2KvZZMbuTBbagjqDgfqj78", que necesitamos conocer para poder enviar bitcoins a una determinada billetera. El proceso de creación de una dirección Bitcoin, y su clave privada correspondiente, se lleva a cabo a través del cliente Bitcoin.

CLAVE PRIVADA: es aquella asociada a una dirección Bitcoin pública, y que permite enviar bitcoins que hayan sido recibidos previamente en dicha dirección.

TRANSACCIÓN: es una declaración pública firmada con la clave privada correspondiente a una dirección Bitcoin. Esto equivale a dejar constancia de que se ha transferido el control sobre la cantidad de bitcoins (o fracción de bitcoin) especificada a otra/s dirección/es.

RED BITCOIN: es una red de ordenadores (nodos) a través de la cual se difunden todas las transacciones Bitcoin y se mantiene la cadena de bloques.

CADENA DE BLOQUES: es una lista pública de todas las transacciones que se han llevado a cabo, gracias a la cual todos los dueños de bitcoins pueden demostrar que lo son. Cada nodo de la red Bitcoin tiene una copia de la cadena de bloques.

BLOQUES: las transacciones se agrupan en trozos grandes de datos llamados bloques. Estos están unidos entre sí de manera tal que cada uno prueba que el bloque anterior es válido, y así forman la cadena de bloques. Como cada bloque contiene el hash del bloque previo, nadie puede quitar o modificar bloques sin que esto sea detectado por la red. La creación de bloques es el trabajo de los mineros, un trabajo que el protocolo de Bitcoin hace deliberadamente difícil, para prevenir que alguien pueda gastar bitcoins y luego crear y distribuir su propia *cadena de bloques* en donde no figure dicha transacción – lo cual le daría la posibilidad de gastarlos nuevamente. Cuando un bloque válido es creado, es distribuido a través de la red y se comienza el trabajo para crear el próximo bloque.

BLOQUE GÉNESIS: es el primer bloque de la cadena, y fue creado el 4 de enero de 2009.

TRANSACCIÓN SIN CONFIRMAR: es aquella que aún no forma parte de un bloque.

CONFIRMACIÓN: ocurre cuando un bloque de transacciones que es candidato a formar parte de la cadena de bloques es reconocido como válido por la red de mineros

"**6 CONFIRMACIONES**": significa que la transacción pertenece a un bloque y que hay 5 bloques posteriores a éste en la cadena. Esto provee una mayor seguridad de que dicha transacción es legítima y, en la práctica, irreversible.

MINERO: es alguien que intenta crear bloques para agregar a la *cadena* (el término también puede referirse al software dedicado a tal fin). Los mineros son recompensados por su trabajo por el protocolo de Bitcoin, que automáticamente asigna (hoy en día) 25 nuevos bitcoins al minero que cree un bloque válido. Cada 4 años, el premio por bloque disminuye a la mitad.

DIFICULTAD: indica qué tan complicado es crear un nuevo bloque. El ajuste de la dificultad, de acuerdo al poder de cómputo de todos los mineros combinados, le permite a Bitcoin asegurar que sus operaciones matemáticas sean lo suficientemente difíciles como para que el esfuerzo combinado de todos estos mineros resuelva 1 bloque cada aproximadamente 10 minutos.

ATAQUE DEL 51%: es un intento de obtener el poder de bloquear y revertir transacciones Bitcoin a través de la obtención y el uso de un pool computacional lo suficientemente poderoso como para dominar al resto de la red (controlando al menos el 51% de la misma).

DOBLE GASTO: es un intento de enviar los mismos bitcoins dos veces. Los mineros previenen que esto suceda, pero aunque tal ataque es difícil de llevar a cabo, es teóricamente posible, en especial contra usuarios que aceptan transacciones sin confirmar. La probabilidad de ser víctima de un doble gasto disminuye drásticamente con cada confirmación (una confirmación demora, en promedio, diez minutos).

EXCHANGE (o **sitio de *trading***): es un servicio que le permite a los

usuarios comprar y vender bitcoins entre ellos de manera eficiente. Los más populares hasta el momento son MtGox, CryptoXChange, Bitfloor, Cavirtex (Bitcoin por dólares canadienses) e Intersango (Bitcoin por Libras esterlinas). Es importante aclarar que las transacciones realizadas dentro de la misma plataforma de trading no se graban en la cadena de bloques; vale decir que, en rigor, los bitcoins recién quedan en posesión de sus dueños cuando son retirados de allí.

PRECIO DE OFERTA (en inglés: ***"ask" price***): es el precio mínimo al que las personas en un determinado *sitio de trading* están dispuestas a vender sus bitcoins.

PRECIO DE DEMANDA (en inglés: **"bid" price**): es lo máximo que están dispuestos a pagar aquellos que buscan comprar.

VOLÚMEN DE UN SITIO DE TRADING: es el número de unidades monetarias comercializadas durante un período dado.

PROFUNDIDAD DEL MERCADO: es el número de bitcoins que las personas han puesto a la venta en un *sitio de trading*, y que aún no han sido comprados (ya que hasta el momento nadie está dispuesto a pagar su precio).

ESPECULADOR: es alguien que intenta obtener una ganancia de las oscilaciones en el precio del Bitcoin (comprando cuando cree haber identificado un piso y vendiendo cuando cree haber identificado un techo).

ARBITRAJE: es la actividad a través de la cual se intenta obtener una ganancia aprovechando la diferencia de precio que puede darse entre los diferentes *sitios de trading*.

TRADING DE ALTA FRECUENCIA : es la actividad a través de la cual se intenta obtener una ganancia al predecir movimientos del precio en el muy corto plazo.

BURBUJA: ocurre cuando por algún motivo se produce una demanda exacerbada de bitcoins, que condiciona un aumento muy marcado del precio seguido de una caída por falta de "cimientos" para dicha demanda.

TRADING MARGINAL (***margin trading***): es una forma riesgosa de especulación en la que se comercian bitcoins usando dinero prestado (el

apalancamiento es la relación entre el total de dinero en juego y el dinero propio invertido). Permite mayores márgenes de ganancia, pero a riesgo de sufrir una liquidación forzada. Por ejemplo, una caída en el precio de un 20% para un apalancamiento 5 a 1 implicaría la pérdida de todo el dinero invertido. De la misma forma, también es posible usar el trading marginal para apostar en contra de Bitcoin (**venta corta** o ***shorting***): en este caso, se usan bitcoins prestados para comprar dólares, y se gana si el precio del bitcoin baja (lo cual permite recomprar los bitcoins embolsando la diferencia); si, en cambio, el precio sube, se puede sufrir una liquidación.